A BETTER STATE OF WAR:

SURMOUNTING THE ETHICAL CLIFF IN CYBER WARFARE

BY

MAJOR BILLY E. POPE, JR.

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Better State of War: Surmounting The Ethical Cliff In Cyber Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School of Advanced Air And Space Studies,,Air University,,Maxwell Air Force Base,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study analyzes the emergent field of cyber warfare through the lens of commonly-accepted tenets of ethical warfare. By comparing the foundational understanding of concepts that determine the justice of wars (jus ad bellum) and justice in war (jus en bello) with the capabilities cyber warfare offers, this work highlights both causes for concern and opportunities for betterment. The first chapter introduces important contextual information and definitions that frame the arguments to follow. Chapter 2 presents a theoretical overview of ethical warfare from which to build. This overview presents five core tenets: good faith proportionality, non-combatant immunity, last resort, and sovereignty. Chapter 3 builds on this framework by analyzing how cyber warfare affects each of the core concepts introduced above. The fourth chapter presents a case study that tests the theoretical assertions presented elsewhere in the work. Finally, the conclusion offers a platform for further exploration and surmises opinions regarding ethics and cyber warfare.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**92**	

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

MICHAEL V. SMITH, Col, USAF (PhD) (Date)

_____

EVERETT C. DOLMAN, PhD (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Billy Pope is a Cyber Operations Officer in the United States Air Force. He was commissioned through Air Force Reserve Officer Training Corps Detachment 002 at the University of Southern California in 2001. He holds a Bachelor of Science degree in computer science from the University of Redlands, a Master of Human Relations degree from the University of Oklahoma, and a Master of Public Administration degree from Harvard University. During his 12-year career, Major Pope has been assigned to bases within the United States and abroad. He has served in communications and cyber operations capacities at the base, major command, sub-unified command, and theater combatant command levels including multiple deployments in support of Operations Iraqi Freedom and Enduring Freedom. Following his assignment to the School of Advanced Air and Space Studies, Major Pope will assume command of the 81st Communications Squadron at Keesler Air Force Base, Mississippi.

ACKNOWLEDGEMENTS

An entire host of people formed the foundation of this work without ever knowing they were involved. Every boss who pushed me to succeed, every senior non-commissioned officer who challenged me to form logical opinions, and every great friend who was strong enough to let me know when I was wrong played a tremendous part in the success of this project. Without these people, the argument never would have been possible in the first place.

I owe special thanks to a group of professional colleagues who helped root this argument in sound intellectual thoughts and prose. I learned to think strategically from General John Allen and Brigadier General Steven Spano. Without these two incomparable gentlemen I would never have developed the appropriate lens through which this project was conceived. I owe thanks to my colleagues from SAASS Class XXIII. All of them helped forge these arguments by questioning assumptions and trial-testing assertions during our many classroom discussions.

None of this would have come together without the unceasing assistance of my advisor, Colonel Michael V. "Coyote" Smith. Col Smith helped turn broad-brush, nebulous thoughts into finished arguments through patience, persistence, and incredible insight. Col Smith genuinely cares about all of the students he advises. Because of this fact, I will not be content with this project unless it makes him proud.

Finally, and most importantly, this project is dedicated to my wife and our wonderful babies who aren't really babies anymore. Every hour devoted to this work was one I did not spend being a better father and husband. Yet my wife and kids make me feel like the most loved man on earth. I owe every last bit of my success to them.

ABSTRACT

This study analyzes the emergent field of cyber warfare through the lens of commonly-accepted tenets of ethical warfare. By comparing the foundational understanding of concepts that determine the justice of wars (*jus ad bellum*) and justice in war (*jus en bello*) with the capabilities cyber warfare offers, this work highlights both causes for concern and opportunities for betterment. The first chapter introduces important contextual information and definitions that frame the arguments to follow. Chapter 2 presents a theoretical overview of ethical warfare from which to build. This overview presents five core tenets: good faith, proportionality, non-combatant immunity, last resort, and sovereignty. Chapter 3 builds on this framework by analyzing how cyber warfare affects each of the core concepts introduced above. The fourth chapter presents a case study that tests the theoretical assertions presented elsewhere in the work. Finally, the conclusion offers a platform for further exploration and surmises opinions regarding ethics and cyber warfare.

Cyber warfare offers both nagging difficulties that complicate existing ethical warfare standards and exciting opportunities to improve how warfare is carried out. Decision-makers charged with the authority to carry out acts of cyber warfare must understand the technical limitations of the offensive and defensive components of cyber warfare. Even more importantly, these decision-makers must appreciate how their actions in this burgeoning domain help shape emergent norms and standards that will promulgate through the domain.

Cyber warfare has the potential to facilitate effects that were previously only achievable through lethal means. This is an exciting development in terms of ethical warfare. While B.H. Liddell Hart famously proposed the reason for war is to create a better state of peace, cyber warfare offers the potential to create a better state of war.

CONTENTS

Illustrations

Chapter 1

Introduction

Few are willing to brave the disapproval of their fellows, the censure of the colleagues, the wrath of their society. Moral courage is a rarer commodity than bravery in battle or great intelligence. Yet it is the one essential, vital quality for those who seek to change a world that yields most painfully to change.
– Robert F. Kennedy

Cyberspace, the only manmade commons, offers tremendous opportunities for global commerce, interpersonal collaboration, and worldwide connectivity.[1] Information in cyberspace traverses enmeshed networks of devices and people at light speed, sparking ideas, coalescing thoughts, and facilitating transactions.[2] Cyberspace and the instantaneous connections the domain provides have redefined many facets of human life, especially in terms of space and time. Societal and political frameworks are undergoing a transfiguration wherein few relationships are left untouched by the reach and capabilities of electronic connectivity.[3] In other words, cyberspace is, quite literally, changing the world.

This is not the first time technology has revolutionized human interaction. When modern ships first traversed the oceans, they connected disparate civilizations in ways that fundamentally changed the geopolitical landscape. When airplanes took flight they made the world smaller, allowing people to travel across giant swaths of the earth at unthinkable speeds. Air power pioneer, Billy Mitchell, said at the dawn of the air-going age, "In a trice, aircraft have set aside all ideas of

[1] Joseph S. Nye, "Power and National Security in Cyberspace," *America's Cyber Future: Security and Prosperity in the Information Age* 2 (n.d.): 1, accessed January 21, 2014.
[2] *Department of Defense Strategy for Operating in Cyberspace*, July 2011, 2, http://www.defense.gov/news/d20110714cyber.pdf.
[3] Nicco Mele, *The End of Big: How the Internet Makes David the New Goliath*, First edition (New York: St. Martin's Press, 2013), 2.

frontiers."[4] These paradigm shifts choked old methods of global collaboration until the usurped methods became obsolete. Cyberspace is facilitating a similar monumental shift in human interaction today.

Human relations involve both collaboration and conflict. The innovations that improve how we partner with one another oftentimes affect how we wage war. In addition to the beneficial changes described above, for example, transoceanic shipping allowed the United States to send millions of soldiers abroad to fight two world wars. Airplanes were used to deliver atomic weapons—a paradigm shift in their own right—to kill millions of Japanese citizens in the final throes of World War II. Mitchell, commenting on air power in war said, "A new set of rules for the conduct of war will have to be devised and a whole new set of ideas of strategy learned by those charged with the conduct of war."[5] New capabilities drive new definitions of acceptable conduct, new thresholds between tolerable and intolerable acts, and altogether new ethical criteria for decision-makers to consider.

Bold determinations on the efficacy of newly developed, untested technologies can be elusive for even the most seasoned strategic thinkers. For example, consider the circumstances surrounding the initial development and deployment of nuclear weapons. In *Danger and Survival*, former National Security Advisor, McGeorge Bundy, describes the environment of the scientists and policy-makers involved with nuclear development efforts as one of optimism and determination.[6] On President Truman's decision to drop two atomic bombs on Japan, Bundy writes "As far as we know from the accounts of the three men who met at the first major discussion [Truman, Stimson, and Groves], not one of them expressed any doubt that when the bombs were ready, they should

[4] William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military* (Tuscaloosa, AL: University of Alabama Press, 2009), 4.
[5] Mitchell, *Winged Defense*, 6.
[6] McGeorge Bundy, *Danger and Survival: Choices about the Bomb in the First Fifty Years*, 1st ed (New York: Random House, 1988), 55.

be used."[7] These key leaders did not predict that their decision would turn into a fierce ethical debate persisting unresolved to this day.

Dr. George Lucas, a prominent Naval War College philosopher and ethicist at the forefront of this subject said, "When we find ourselves venturing into a new area of relatively unfamiliar terrain like this, the usual advice is to proceed with caution, speak and think carefully, and observe as closely as possible the sorts of behaviors that are actually taking place, and are found to test the limits of minimally acceptable conduct."[8] Cyberspace and the capabilities the new domain provides are still in their infancy. Now is the time to consider how using the domain for war will shape norms of behavior around the world. While skirmishes and low-level conflict continue to permeate cyberspace, the world has yet to witness a full-scale cyber conflict that approaches the scale some experts predict.[9] By framing the ethical debate and addressing the disparity between what we *can* do and what we *should* do, the collective global society has the rare opportunity to contemplate ethical guidelines for cyber warfare before history is replete with examples of unethical employment. The main goal of this paper is to inform this emerging ethical debate.

Definitions

The vocabulary used to describe conflicts and collaboration in this new domain is not yet understood universally. Therefore, before moving forward, key terms used throughout this study deserve specific attention. As transformative as the cyberspace domain is, for example, the concept

---

[7] Bundy, *Danger and Survival*, 59.

[8] *Dr. George R. Lucas, Jr. on Just War and Cyber Conflict Part 2*, 2012, http://www.youtube.com/watch?v=FRdsUwSuYis&feature=youtube_gdata_player.

[9] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on US," *New York Times* 11 (2012), http://moodle2.portage.k12.wi.us/pluginfile.php/21229/mod_resource/content/1/Digital%20Pearl%20Harbor.pdf. In a speech at the Intrepid Sea, Air and Space Museum in New York, Mr. Panetta painted a dire picture of how a cyber-attack on the United States might unfold. He said he was reacting to increasing aggressiveness and technological advances by the nation's adversaries.

of the domain itself is only vaguely defined and even less understood. Cyberspace is not a place. It has no physical address beyond the routers, servers, cables, and computers that form its framework. Yet cyberspace exists *everywhere* in the connections it facilitates between peoples and devices.[10] Cyberspace is constantly referenced in discussions of politics, security, economics, and influence. None of these disciplines defines cyberspace the same way.[11] Additionally, nearly every community with a stake in cyberspace, from technophiles to elected officials, contextualizes the domain in a unique way. The International Telecommunications Union, under the auspices of the United Nations, for instance, held a multi-national assembly in Dubai in November 2012 that focused exclusively on how the international community defines and governs cyberspace. The assembly failed to reach consensus, sending the international partners back to their home countries with even less clarity than they started with.[12]

In 2006 the Chairman of the U.S. Joint Chiefs of Staff released the National Military Strategy for Cyberspace Operations. The strategy defined cyberspace as "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure."[13] The Department of Defense altered its definition of cyberspace in 2008, calling it "a global domain within the information environment consisting

---

[10] *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012), 214.

[11] See, for example, three sets of definitions that focus on different ontological roots for the realm of cyberspace, from openness and oneness to a partitioned environment of safeguards facilitated by electronic controls. *U.S National Military Strategy for Cyberspace Operations*, 2006, 6, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf; Christopher Castellino, "Defense Department Adopts New Definition of 'Cyberspace,'" *Inside the Air Force*, May 23, 2008, http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm; Rain Ottis and Peeter Lorents, "Cyberspace: Definition and Implications," *Proceedings of the 5th International Conference on Information Warfare and Security*, 2010, 267–70.

[12] *World Telecommunication Standardization Assembly Resolution 50 - Cybersecurity*, Resplution (International Telecommunications Union, n.d.), 1, http://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2050.pdf.

[13] *U.S National Military Strategy for Cyberspace Operations*, 6.

of the interdependent network of information technology infrastructures, including the Internet, telecommunications network, computer systems, and embedded processors and controllers."[14] While the new definition still clings to the technical roots of computer science and networking, it notably infers a more cognitive basis of cyberspace in the information realm. Cyberspace is more than a collection of interconnected electronic devices and processors. The networks and peripherals that connect people together in cyberspace form the medium, but cyberspace more closely resembles a complex nervous system than a sterile electronic array. As cyberspace continues to root itself, its reach and entanglement in the more traditional domains make it a powerful influence on existing societal structures. Cyberspace is not just a *quantitatively* different environment that builds upon traditional understanding. Cyberspace is a *qualitatively* different realm that does not lend itself to strategic paradigms from other operating environments.

The nature of cyberspace continues to evolve away from its technical underpinnings toward its cultural implications. In 2011 President Barrack Obama released the International Strategy for Cyberspace. The White House's interpretation of the cyber realm further pushes contemporary thinking on cyberspace away from its computer-networking roots into a more humanistic, interpersonal context. The report states "The cyberspace environment that we seek rewards innovation and empowers individuals; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security.[15]" In this context, cyberspace becomes an independent arena for thought and action that is

[14] Christopher Castellino, "Defense Department Adopts New Definition of 'Cyberspace.'"
[15] United States White House Office and Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked Worldr* (White House, 2011), 8–9, http://scholar.google.com/scholar?cluster=13455456761010981645&hl=en&oi=scholarr.

altogether distinct from its physical counterparts on land, at sea, in the air, and in space.

While it is noble to seek a cyberspace environment that promotes cooperation and innovation, we must acknowledge the dark, transgressive side of this burgeoning domain. The antithesis of the mutually beneficial environment we seek is a cyberspace where competition and fear overshadow collaboration. Hobbes, in his fundamental law of nature, warns, "That every man, ought to endeavour Peace, as farre as he has hope of obtaining it; and when he cannot obtain it, that he may seek, and use, all helps and advantages of Warre."[16] Cyberspace will continue to civilize. As the domain matures, however, so too will the methods of malefactors who upset collective attempts at peace in favor of conflict.

Cyber warfare is an oft-debated term that is central to the discussion that follows. Richard Clarke, a widely regarded homeland security and cyber security expert who advised three US presidents, defines cyber warfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[17] This definition, however, is overly restrictive in the way it limits who can be considered combatants in cyberspace. Cyberspace empowers individuals and non-state actors in ways the physical domains cannot. In his 2013 book, *The End of Big,* Harvard lecturer and digital strategist Nicco Mele writes "Today, national security is fragile, with power shifting to technologically-equipped terrorist groups, revolutionary movements, criminal enterprises, murky collectives such as Anonymous, and even isolated individuals with an Internet connection."[18] This newfound power can be used to promote peace, but it is also cause to

[16] Thomas Hobbes, *Leviathan*, Rev. student ed, Cambridge Texts in the History of Political Thought (Cambridge ; New York: Cambridge University Press, 1996), 92.
[17] Richard A. Clarke, *Cyber War: The next Threat to National Security and What to Do about It*, 1st Ecco pbk. ed (New York: Ecco, 2012), 6.
[18] Mele, *The End of Big*, 155.

rethink the boundaries we place around the concept of warfare in cyberspace. By limiting participants to only those of recognized nation-states we inappropriately constrain the field of cyber warfare.

Jeffrey Carr, author of *Inside Cyber Warfare*, summons the spirit of Sun Tzu in his definition of cyber warfare, saying it is "the art and science of fighting without fighting; of defeating an opponent without spilling their blood."[19] While this interpretation certainly broadens the definition sufficiently to encompass actions by both state and non-state actors, it unnecessarily opens the aperture for what should be considered acts of cyber warfare. If the target of cyber aggression is a commercial enterprise, for instance, a more appropriate label for the action might be cyber-crime. Cyber warfare aims to influence policy and power. The interpretations presented above, combined with Carl von Clausewitz's assertion that war is a continuation of policy, yields the definition of cyber warfare used through the rest of this paper: Actions by state or non-state actors that exploit an adversary's information systems in order to further political objectives.

If cyber warfare is a unique form of warfare, it deserves close examination unencumbered by traditional doctrine, rules, and laws. Cyber warfare enhances land, sea, air, and space power but it also offers altogether new capabilities. Consider the following example highlighting how cyber capabilities changed the face of air power in less than two decades. When the United States repelled Iraq's invasion of Kuwait in 1991, the American Air Force disabled Iraq's integrated air defense system by permanently destroying radar sites, anti-aircraft systems, and electrical switching stations.[20] In 2007, the Israeli Air Force penetrated Syrian airspace en route to an alleged nuclear reactor at Dier-ez-Zor. Israeli pilots simply flew past Syria's air defense systems undetected.

---

[19] Jeffrey Carr, *Inside Cyber Warfare*, 2nd ed (Beijing ; Sebastopol, CA: O'Reilly, 2012), 2.

[20] Michael R Gordon and Trainor, *The Generals' War: The inside Story of the Conflict in the Gulf* (Boston: Little, Brown, 1995), 112.

While Israeli officials have never confirmed the details of this operation, it is widely accepted that a cyber-attack blinded the air defense systems, achieving the desired effect, while preserving the systems and their associated personnel from physical destruction.[21] Significant questions regarding the character and nature of war emerge when targets can be turned off and on rather than being destroyed.

Finally, it is worthwhile to draw distinction between the terms *ethics* and *morality* as they appear in the academic resources that form the basis of the argument that follows. Morality, generally defined as that which governs right and wrong, is a term that seldom appears in isolation without some form of caveat or delineator.[22] Christian morality, for instance, defines moral principles within the parameters established by the Bible.[23] Political scientists grapple with terms like *realist morality* when exploring international norms and standards.[24] The Stanford Encyclopedia of Philosophy recognizes this tendency and suggests morality can be both a term that describes attributes of a particular group or society, or it can be a normative term that applies to all rational humans.[25] Michael Walzer grounds this concept in terms applicable to this study when he asserts, "It is important to stress that the moral reality of war is not fixed by the actual activities of soldiers but by the opinions of mankind."[26] This work infers morality to be a guiding philosophical concept that differentiates between right and wrong at a foundational level. This study acknowledges the logic behind Hobbes' sentiment, however, when he writes "For one man calleth *Wisdome*, what

[21] Charles W. Douglass, *21st Century Cyber Security: Legal Authorities and Requirements*, Strategic Research Project (U.S. Army War College, March 22, 2012), 14.
[22] Oxford English Dictionary, *Oxford English Dictionary Online* (Oxford University Press, Oxford, UK http://www. oed. com, 2008), http://scholar.google.com/scholar?cluster=5447292547848391191&hl=en&oi=scholarr.
[23] *Peace, Politics, and the People of God* (Philadelphia: Fortress Press, 1986), 117.
[24] Justin Cruickshank, *Critical Realism: The Difference It Makes* (Routledge, 2003), 31.
[25] Bernard Gert, "The Definition of Morality," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Fall 2012, 2012, http://plato.stanford.edu/archives/fall2012/entries/morality-definition/.
[26] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 4th ed (New York: Basic Books, 2006), 15.

another calleth *feare*; and one *cruelty*, what another *justice*; one *prodigality*, what another *magnanimity…"*[27] Moral considerations and interpretations, therefore, may differ across societies or communities depending on how right and wrong are perceived.

Ethics, on the other hand, is by and large considered to be a branch of knowledge that deals with moral principles.[28] Ethics, in this interpretation, is the study of morality along with its circumstances, context, and aggregative features. Academic and professional communities routinely adopt ethical standards. Medical ethics, for example, govern the professional and moral standards of medical practitioners.[29] This paper adopts an interpretation of ethics that emphasizes the professional nuance related to the term. While the arguments presented throughout this work deal with both morality and the ethical structures that frame and interpret morals, the vocabulary used herein is chosen carefully. This work will focus on the ethics of warfare and the ethics of cyber warfare as collections of moral principles interpreted through the lens of the profession of arms.

Limitations

The fact that a full-scale employment of cyber warfare remains only a theoretical possibility is a good thing. Cyber warfare is capable of causing grave harm to the world's citizenry and its nation states.[30] However, the absence of historical evidence and precedents creates difficulties for academics and practitioners studying the implications of this field. One can easily look to history to determine how machine

[27] Hobbes, *Leviathan*, 31.
[28] Dictionary, *Oxford English Dictionary Online*. One definition of ethics presented in the Oxford Dictionary makes the term nearly synonymous with *morality* while a second definition creates the understanding that ethics contains the study of morality in a given context.
[29] American Medical Association, *Principles of Medical Ethics of the American Medical Association* (American Medical Association Press, 1903), Preface.
[30] Clarke, *Cyber War*, 2012, 104. Clarke describes how the capabilities known to exist in the US arsenal of cyber weapons would impact the United States if its adversaries had similar weaponry and access.

guns, nuclear weapons, and poisonous gasses changed perceptions of war because all three were used in combat. The reactions to each and the ensuing ethical debates helped construct the ethical norms we employ today. Without this historical guidance, the ethical construct for cyber warfare will remain, at best, notional. For the sake of humanity, let us all hope it remains as such.

The concepts of anonymity and attribution together form another limitation this study must endure. It is easy for actors in cyberspace today to remain anonymous if they chose to do so. Encryption technologies allow even unsophisticated actors in cyberspace to do a relatively good job of covering their tracks.[31] Nation-states and well-resourced non-state actors have even more advanced capabilities that allow them to remain anonymous online. These factors, coupled with the monetary and computing resources required to record the actions of individual people in cyberspace make attribution incredibly difficult. Therefore, even actors who make little effort to be anonymous are likely to remain undetected anyway.

These attribution and anonymity problems create limitations to this study because they decrease the available evidence associated with the low-scale acts of cyber war that have taken place. Anonymity, and the effect it has on the ethics of cyber warfare, will be discussed later. The important point here is that anonymity also limits the depth of evidence available for academic research.

Methodology and Evidence

The ethics of warfare have been studied and documented almost continuously since Thucydides wrote about the Peloponnesian War in

[31] Dan Goodin, "Scientists Detect 'spoiled Onions' Trying to Sabotage Tor Privacy Network," *Ars Technica*, January 21, 2014, http://arstechnica.com/security/2014/01/scientists-detect-spoiled-onions-trying-to-sabotage-tor-privacy-network/. Tor is a widely available software client that allows anyone with a computer to traverse cyberspace anonymously using commercial-class encryption.

431 BC[32] Academic research on the ethics of *cyber* warfare, however, is only now starting to reach publication. This paper will build on the mature tenets of the existing just-war ethic where logically sound comparisons can be made. Commonly accepted attributes of just-war theory such as non-combatant immunity and proportionality form a strong foundation from which to build arguments relevant to the ethics of cyber warfare. The next chapter will establish a framework of ethics and war. The concepts presented in Chapter Two are drawn from sound military, political, and philosophical sources that collectively form the just-war ethic as we know it today.

One should caution against the temptation to transpose ethical standards directly from traditional forms of warfare to cyber warfare without closely examining the specific criteria used to justify each application. Cyber warfare is unique. The ethical norms of traditional warfare serve as sound points of departure but they are not sufficient. Chapter Three will build upon our basic ethical war framework, aligning with accepted standards where appropriate and departing from these ideas where required. Current events drawn from a host of professional journals and media outlets, combined with a fledgling collection of theory on cyber warfare, will form the evidentiary base for ethical proposals specific to cyber warfare.

Finally, Chapter Four will explore how the concepts developed in the third chapter apply to a hypothetical cyber warfare case study. With only limited historical evidence, direct application of this theory is difficult. Current understanding of the capabilities and limitations of cyber warfare paint a reasonably clear picture of what cyber warfare might entail. This scenario will serve as a proving ground for ethical concepts developed throughout the rest of this work.

---

[32] Thucydides, *History of the Peloponnesian War*, [Rev. ed, The Penguin Classics (Harmondsworth, Eng., Baltimore]: Penguin Books, 1972). Thucydides offers several examples of *might versus right* through the course of the war, including The Mytilenian Debate and the Melian Dialogue.

Cyberspace is pervasive. As the global society becomes increasingly dependent upon the advances cyberspace offers, ethical standards and norms become even more vital. This work intends to inform the emerging ethical debate in hopes of encouraging standards for the betterment of a globally interconnected society.

Chapter 2

An Ethical Framework of War

On the surface it seems counterintuitive to study ethics and warfare in the same space – the same cosmos of thought. Maybe two ideas that appear diametrically opposed ought to be kept that way. Ethics, that which pertains to the ideals of right and wrong, seems to have very little overlap with a nasty, brutish thing like war. While one party lobbies for cooperative peace, the other sharpens its daggers. However, these two spheres overlap in surprising and unexpected ways. Take for instance war that is intended to return conquered people to freedom. Consider war that is fought for purely defensive reasons. People fighting for their own survival seem quite justified in taking up arms to do so.

James Childress uses the example of early Christians to illustrate the logjam between pacifism and war.[1] Childress cites Christian teachings, especially the Sermon on the Mount, as ethically binding requirements for Christians to oppose the ghastly practices of bloodshed in war. He carries the debate forward, however, by reframing the simplistic description of *pacifism* from "opposition to war" into a more provocative definition of the term: "making peace."[2] In doing so, Childress opens the door to the possibility that war may be required in order to create peace. Military theorists in the vein of B.H. Liddell Hart echo similar sentiments. Liddell Hart says "The object in war is a better state of peace….Hence it is essential to conduct war with constant regard to the peace you desire."[3]

---

[1] James Childress is the John Allen Hollingsworth Professor of Ethics at the University of Virginia Institute for Practical Ethics and Public Life. In 2004, Childress received the Lifetime Achievement Award from the American Society of Bioethics and Humanities.

[2] *Peace, Politics, and the People of God* (Philadelphia: Fortress Press, 1986), 118.

[3] Basil Henry Liddell Hart, *Strategy*, 2nd rev. ed (New York, N.Y., U.S.A: Meridian, 1991), 338.

If the duty of pacifism is to create peace, the pacifist finds himself in a dilemma that requires close examination of the type of peace desired. Peace on someone else's terms requires only acquiescence, but self-determined *peace* must be protected from *evil* forces that threaten it. William Frankena extrapolates Childress's position on peace by relating it to "beneficence," or active goodness.[4] Frankena suggests man is obligated to create peace for his fellow man through four levels of beneficence: (1) by *not inflicting evil*, (2) by *preventing evil*, (3) by *removing evil*, and (4) by *promoting good*.[5] Frankena's interpretation suggests peace is an active state that requires maintenance. Peace, in the face of evil, may require the use of force.

In the face of an unrelenting enemy, war surfaces as the ethical alternative to forfeiture of life and values. Childress calls responsibilities that harbor strong moral reasons for their performance *prima-facie* obligations.[6] For example, the idea that a man should not kill or injure another man is a *prima-facie* concern. When this *prima-facie* obligation conflicts with the moral requirement to protect people from evil, reasoning and justification are required.[7] Childress writes, "But if one does not misconstrue peace as the total absence of conflict, one can see how the *prima-facie* obligation not to injure or kill others persists even in the midst of war by mandating the ultimate objective of peace. And through the object of peace…it imposes other restraints on the conduct of war."[8] If one can agree that evil exists, one must also consider man's responsibility to counter evil. Frankena outlines ethical responsibilities

[4] William K. Frankena was an American moral philosopher. He was a member of the University of Michigan's department of philosophy for 41 years, and chair of the department for 14 years. Frankena published several books on ethics and morality including *Ethics* (1988) and *Perspectives on Morality: Essays* (1977).
[5] William K. Frankena, *Ethics*, 2d ed, Prentice-Hall Foundations of Philosophy Series (Englewood Cliffs, N.J: Prentice-Hall, 1973), 47.
[6] James Childress, "Just-War Theories: The Bases, Interrelations, Priorities and Functions for Their Criteria," *Theological Studies* 39, no. 3 (1978): 430.
[7] Childress, "Just-War Theories: The Bases, Interrelations, Priorities and Functions for Their Criteria," 432.
[8] Childress, "Just-War Theories: The Bases, Interrelations, Priorities and Functions for Their Criteria," 439.

in his beneficence levels 2, 3, and 4 that require steadfast resistance and measured force. While some methods of force may be interpreted as evil in and of themselves, others are vindicated when all feasible alternatives fail. Man has a requirement to create and protect peace and this sometimes requires war.

Realists counter this argument by questioning the motivations of the actors involved. Waltz, for example, argues that man only cooperates with fellow men in so far as "life takes priority over justice."[9] Hobbes certainly paints a bleak picture of societal cooperation when he insists life, in the absence of agreed tepid collaboration, is bound to be "solitary, poore [sic], nasty, brutish, and short."[10] J.F.C. Fuller, a lifelong military theorist and practitioner, wrote "We frequently hear the assertion made that man has a right to live. In spite of the humanitarians, natural man, I hold, has no right to live, but, possessing power to protect his life, his might becomes the right to safeguard it."[11] Contrary to Childress's interpretation, realists suggest man's self-interest drives him toward a cooperative state, regardless of his desire for greater peace. While Childress might interpret the cause of a war as a desire for better society, Waltz and other realists could interpret the same conflict as one fought to ensure survival, regardless of any ethical predisposition.

Yet as long as historians and philosophers have been writing and thinking about war, they have also been considering whether its practice and methods are right and just. Michael Walzer, discussing what he calls "Historical Relativism," summarizes this concept brilliantly, saying "Even when world views and high ideals have been abandoned—as the glorification of aristocratic chivalry was abandoned in early moderns times—notions about right and wrong conduct are remarkably

[9] Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 2001), 172.
[10] Hobbes, *Leviathan*, 88.
[11] J.F.C. Fuller, *The Foundations of the Science of War* (Books Express, 2012), 59.

persistent: the military code survives the death of warrior idealism."[12] If the pure realists and Hobbesians are correct in their interpretation that war simply falls outside the moral universe of right and wrong, the debate ends here. However, if Thucydides's agony over the Athenians' decision to attack Melos in 430 B.C was justified we have cause to ponder this topic.[13] If Clausewitz's careful coupling of violence and policy hundreds of years later offers any indication, military acts, by nature, include ethical components.[14] Michael Walzer warns, "*War* is hell."[15] Yet if situations exist where war becomes the only viable option for otherwise peaceful people, we must consider the ethics of war, or *jus ad bellum.*[16]

Therefore, the crevasse between war and ethics is much smaller than it appears at first pass. Unless we assume righteousness will naturally prevail over evil without man's intervention, wars may become necessary. Furthermore, the justification for certain wars can be founded on completely ethical terms. The work of the strategist, policy-maker, and average citizen is in not to determine *whether* war is just, but to surmise *which* wars are just and unjust. Considering ethical differences brought about by motivations, cultures, religions, and capabilities, the task of differentiating between just war and unethical violence is a difficult task indeed.

Ethical judgment does not end when one determines a war is justified. The methods used in war, *jus en bello*, are also subject to fierce debate. Perhaps even more important than whether wars are fought is

---

[12] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 4th ed (New York: Basic Books, 2006), 16.

[13] Thucydides, *History of the Peloponnesian War*, 1972, 403–405. The Melian dialog carefully captures the debate between Melos and Athens over whether an attack against Melos was justified given the inability of Melos to resist.

[14] Carl Von Clausewitz, Michael Howard, and Peter Paret, *On War* (Princeton: Princeton University Press, 2011), 89, http://site.ebrary.com/id/10578581. Clausewitz is careful to delineate acts of war from primordial violence in his "three tendencies" that underpin war.

[15] Walzer, *Just and Unjust Wars*, 21.

[16] Walzer, *Just and Unjust Wars*, 21.

the question of *how* they are fought. The first recorded restraints placed on the use of force that limited raw military capabilities stemmed from Gratian's compilation of canon law.[17] One of the early canonical principles, the Truce of God, originally prohibited Christians from fighting on Sundays. By the 11th century, the ban as it was written extended to include most Christian festivals. While history is replete with instances where the ban was ignored or reinterpreted to allow certain types of warfare to occur on holy days, the existence of ethical limitations within the conduct of war is significant.[18]

Jus en bello also incorporates the idea that certain weapons are too brutal or non-discriminate to ethically employ in war. An additional stipulation within the Truce of God prohibited Christians from employing the crossbow in combat.[19] Chemical weapons like mustard gas, biological agents such as anthrax and cholera, and nuclear weapons killed hundreds of thousands of people on battlefields in both World Wars.[20] One of the more prominent reasons these weapons were developed was to counter the ever-increasing lethality of more traditional weaponry. For example, one noted justification for the nuclear bombs dropped on Hiroshima and Nagasaki was that the enormous weapons shortened the war and saved lives that would have been lost in a more conventional invasion of mainland Japan.[21] Following periods of relative acceptance immediately after their creation, however, all three of these types of weapons were admonished by the international community.[22]

---

[17] James Turner Johnson, *Just War Tradition and the Restraint of War: A Moral and Historical Inquiry* (Princeton, N.J: Princeton University Press, 1981), 124–125.
[18] Johnson, *Just War Tradition and the Restraint of War*, 127.
[19] Johnson, *Just War Tradition and the Restraint of War*, 128.
[20] Friedrich Frischknecht, "The History of Biological Warfare," *EMBO Reports* 4, no. Suppl 1 (June 2003): 48, doi:10.1038/sj.embor.embor849.
[21] Bundy, *Danger and Survival*, 89.
[22] "Chemical and Biological Weapons - ICRC," 00:00:00.0, http://www.icrc.org/eng/war-and-law/weapons/chemical-biological-weapons/overview-chemical-biological-weapons.htm.The Geneva Protocol of 1925 banned the use of chemical and biological weapons. Measures to further strengthen the ban were enacted in 1972 and 1993. International legislation on the use, testing, and proliferation of

Several components of just war theory related to *jus en bello* and *jus ad bellum* are critical to the arguments that follow in subsequent chapters and deserve further development here. Childress deduced five ethical components common to most modern conflicts that deserve specific examination. These factors will play a significant role in the discussion to follow regarding ethics in the emerging battlefields of cyberspace. The five components are:[23]

1. Good faith. When "perfidy, bad faith, and treachery" are prevalent on the battlefield, restoring and maintaining peace becomes difficult. The ethical imperative of good faith insists *prima-facie* obligations invoke the responsibility to treat one's enemies humanely.[24] Enemy soldiers are combatants who may justifiably be killed. Yet when combatants are captured or wounded, rendering them unable to continue fighting, they should be treated humanely.[25] Torture, maltreatment, and withheld medical care undermine the good faith premise. Without this premise, combatants understandably will continue fighting at all costs to avoid heinous consequences at the mercy of a treacherous enemy. If the assurance of good faith disappears, so does any incentive for an incapacitated enemy to surrender.

2. Non-combatant Immunity. In 1940 Dr. John K. Ryan popularized the sentiment that combatants and non-combatants should expect different treatment in times of war. Ryan wrote "First, there is an essential moral distinction between innocent non-combatants and guilty combatants; second, the latter can be directly put to death during the war and even, in certain cases, after the war, while innocent non-

---

nuclear materials was prominent throughout the Cold War and continues to affect international relations today.

[23] Childress, "Just-War Theories: The Bases, Interrelations, Priorities and Functions for Their Criteria," 439–442.

[24] Childress, "Just-War Theories: The Bases, Interrelations, Priorities and Functions for Their Criteria," 440.

[25] Walzer, *Just and Unjust Wars*, 138.

combatants can be at most only indirectly put to death."[26] Similarly, Walzer writes, "soldiers as a class are set apart from the world of peaceful activity; they are trained to fight, provided with weapons, required to fight on command. No doubt, they do not always fight; nor is war their personal enterprise. But it is the enterprise of their class, and this fact radically distinguishes the individual soldier from the civilians he leaves behind."[27] The separation between combatants and non-combatants hearkens back to *prima-facie* obligations against harming or killing innocent people. It proposes a framework that limits combat to those who have chosen to take up arms, leaving other citizens free from the perils of war.

In modern war, one must consider who is and who is not a combatant. In total war, for instance, entire societies provide resources in manpower, supplies, and funds to wartime efforts. Childress describes the distinction between combatants and non-combatants as "contextual and thus partially determined by the society and the type of war."[28] Irregular warfare techniques like guerilla warfare and terrorism often make basic differentiation between innocent citizens and warfighters extremely difficult.[29] As late as World War I, armies isolated themselves on secluded battlefields and fought each other in easily identifiable struggles. Today, with deep battle capabilities and asymmetric techniques, combatants are much less distinct.

Some potential targets in war, however, are both civilian and military in nature. In Operation Desert Storm, for example, one of the first targets specified in John Warden's air campaign was Iraq's electrical grid.[30] Integrated air defense systems and Iraq's command and control

---

[26] John Ryan, *Modern War and Basic Ethics* (Milwaukee: WI Bruce Publ Co, 1940), 35.
[27] Walzer, *Just and Unjust Wars*, 144.
[28] Childress, "Just-War Theories: The Bases, Interrelations, Priorities and Functions for Their Criteria," 440.
[29] *Understanding Modern Warfare* (Cambridge ; New York: Cambridge University Press, 2008), 234–236.
[30] John Andreas Olsen, *John Warden and the Renaissance of American Air Power*, 1st ed (Washington, D.C: Potomac Books, 2007), 149.

capabilities were inherently dependent upon electricity. Warden's effects-based targeting scheme made the electrical grid a viable military target. However, hospitals, businesses, and residences were also completely reliant on electricity provided through the same grid. Walzer suggests the ethical burden in this instance rests with the actors involved to prove their intent was a means to an acceptable effect rather than a retributive measure aiming to effect non-combatants themselves.[31]

Some scholars argue that dual-use targets are simply off-limits if wars are to be fought on ethical grounds. In an article titled *The Morality of Obliteration Bombing,* John Ford argues "The principle moral problem raised by obliteration bombing, then, is that of the rights of non-combatants to their lives in war."[32] Fire bombing raids on Tokyo and Dresden during World War II, for example, are often judged as ethically illegitimate, regardless of the military advantage they produced.[33] It is certainly difficult to imagine Liddell Hart's "better peace" emerging from a war when entire cities and societies are destroyed while creating said peace.

3. Proportionality. Proportionality in this study suggests the amount of force used to subdue an enemy should be held to the minimum in order to reduce unintentional harm to non-combatants. Laser and satellite guided munitions like those delivered by aircraft in Operations Desert Storm, Iraqi Freedom, and Enduring Freedom, for instance, are capable of delivering highly accurate and selective lethal force, even in urban environments.[34] The responsibility for such precision stems from the ethical obligation to limit non-combatant deaths.

---

[31] Walzer, *Just and Unjust Wars*, 153.
[32] John Ford, "The Morality of Obliteration Bombing," *Theological Studies* 5 (1944): 269.
[33] Ford, "The Morality of Obliteration Bombing," 264, 271.
[34] Benjamin S. Lambeth, *The Unseen War: Allied Air Power and the Takedown of Saddam Hussein* (Annapolis, Md: Naval Institute Press, 2013), 91.

Going far beyond a simple chivalric responsibility, proportionality serves the practical purpose of selectively engaging combatants when they are surrounded by non-combatants. This level of discrimination helps to ensure neutral or friendly non-combatants remain as such. When means of warfare cause civilian harm and are perceived to be disproportionate in nature, new enemies are created that may otherwise have remained disengaged from the war effort.[35] Thucydides, describing the Athenians' ruthless assault on Corcyra, provides a telling historical example. The Athenians adopted a course of warfare that included revenge killings and needless slaughter. Thucydides wrote, "there were the savage and pitiless actions into which men were carried not so much for the sake of gain as because they were swept away into an internecine struggle by their ungovernable passions."[36] The citizens of Corcyra who witnessed these events and survived dedicated their lives to the forces united against Athens.[37]

Nuclear targeting provides the quintessential case study for the ethical boundaries of proportionality. It's hard to imagine a scenario in which a weapon capable of destroying an entire city could be considered proportionate to a dissimilar military threat. Nuclear weapons cannot discern between combatants and non-combatants. Yet great minds like Thomas Schelling argue that the value of nuclear weapons is not in their use, but in their potential – their *non*-use.[38] Nuclear weapons are so terrifyingly lethal that they have produced a perverse peace in which assured nuclear retaliation begets nuclear aggression.[39] Kant's theory of international politics, for instance, suggests states may learn enough

[35] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (New York: Oxford University Press, 2011), 35.
[36] Thucydides, *History of the Peloponnesian War*, [Rev. ed, The Penguin Classics (Harmondsworth, Eng., Baltimore]: Penguin Books, 1972), 244–245.
[37] Thucydides, *History of the Peloponnesian War*, 1972, 246.
[38] Thomas Schelling, "An Astonishing Sixty Years: The Legacy of Hiroshima," *The American Economic Review*, September 2006, 929.
[39] Schelling, "An Astonishing Sixty Years: The Legacy of Hiroshima," 932.

from the suffering and devastation of war to adhere voluntarily to an ordered, relatively peaceful coexistence.[40] An ethical argument can be made, therefore, that a carefully managed nuclear balance helps maintain a healthy strategic environment, thereby preserving the lives that would be lost if nuclear weapons were unleashed.[41]

4. Last Resort. *Jus ad bellum* rests on the bedrock assumption that all feasible alternatives short of war have been exhausted before resorting to the use of force.[42] Diplomatic alternatives, economic pressures, and even threats of violence backed by supporting military capabilities have all shown to be effective to some degree at dispelling tension or coercing adversaries.[43] Considering options short of war also upholds the *prima-facie* obligation against doing unnecessary harm.

Two wars that, when compared, exemplify the notion of last resort are the United States' 1991 and 2003 engagement in Iraq. In 1991, the United States went to great diplomatic lengths to persuade Saddam Hussein to withdraw his forces from Kuwait after he aggressively invaded the country. After months of negotiations and pressure, the United States issued a final ultimatum to withdraw, leaving a full forty-eight hours for Iraq's leadership to facilitate the removal of their forces from Kuwaiti soil. When the final ultimatum was ignored, leaving Kuwaiti citizens under illegitimate oppression, the Iraqis were driven from Kuwait by force.[44] On the contrary, America's preventative war with Iraq in 2003 rested on assumptions that Iraq and its associates posed a dire threat to the United States, regardless of their intentions to immediately launch an attack. Richard Haass, a presidential advisor during both wars, called the 1991 Gulf War a "war of necessity" and the 2003 conflict

[40] Waltz, *Man, the State, and War*, 164.
[41] Schelling, "An Astonishing Sixty Years: The Legacy of Hiroshima," 933.
[42] Walzer, *Just and Unjust Wars*, 211–212.
[43] Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed (New York: Longman, 1999), 390–391.
[44] Lawrence Freedman and Efraim Karsh, *The Gulf Conflict, 1990-1991: Diplomacy and War in the New World Order* (London: Faber and Faber, 1994), 233.

"a war of choice."[45] The chasm between prevention and preemption – necessity and choice - requires significant ethical debate.

An alternative definition of last resort suggests war should be the least desirable course of action, but not necessarily the last choice. Israel's preemptive participation in the Six Day War of 1967 offers a counter example that illustrates what Walzer calls "a clear case of legitimate anticipation."[46] Several Israeli intelligence sources and diplomatic outlets corroborated reports that overwhelming Egyptian military power was amassed to invade Israel. The ensuing Israeli surprise attack against the Egyptians was most certainly not conducted once all other options were tried. However, history reflects positively on the attack as a justified use of offensive military power for necessary self-defense.[47]

The concept of last resort, however it is defined, is one that rests on solid ethical ground. Just war theory precludes aggression. Any instance where feasible options short of war are foregone or ignored introduces the distinct possibility that aggressive intentions underpin one's actions. However, when threats overrun otherwise peaceful and cooperative alternatives, justified force may emerge as the most reasonable course of action.

5. Intervention/ Sovereignty. The final component of just war theory that deserves specific mention in this study involves the sanctity of state sovereignty juxtaposed with the requirement to promote peace. Beginning with the Peace of Westphalia in the mid 1600's the world's political landscape continually evolved into an interconnected web of sovereign states.[48] While international institutions like the United Nations and its predecessor, the League of Nations, have attempted to

[45] Richard Haass, *War of Necessity: War of Choice* (New York: Simon & Schuster, 2009), 11.
[46] Walzer, *Just and Unjust Wars*, 85.
[47] Walzer, *Just and Unjust Wars*, 84.
[48] Robert W. Cox, *Approaches to World Order*, Cambridge Studies in International Relations 40 (Cambridge ; New York: Cambridge University Press, 1996), 494.

govern inter-state relations, no world order has emerged as of yet to trump the system of geographically separate, self-governing nation-states.[49] Alliances and coalitions help maintain stability by balancing world power. However, no organizational element has the viability of each individual country. Strong international norms and legal parameters require a high threshold of justification for violation of state sovereignty. Walzer places such a high importance on sovereignty that he suggests it can only be breached in response to "acts that shock the moral conscience of mankind."[50]

Sovereignty, however, creates a *prima-facie* dilemma when the leadership of a country is either incapable of protecting its citizens or it becomes a source of inhumane treatment. One must weigh justice versus life if one desires to create peace where sovereignty acts as a barrier. Natural law theorists, for example, believe human beings have the moral obligation to protect other humans from harm, regardless of existing structures, norms, or guidelines.[51] Relatively weak nations and classicists, on the other hand, argue that intervention usually occurs when a powerful culture wishes to impose its ideals and norms on the less powerful.[52] A situation one nation perceives as a moral crisis requiring intervention may simply be the status quo or a cultural norm to another.

Walzer's idea justifying intervention in situations that shock the human conscience, however, is powerful indeed. Certainly, high thresholds are necessary to prevent the subversion of sovereignty at the whim of powerful nations. Standards of acceptability and human rights are difficult to generalize. As Jack Donnelly observes, "Just as in domestic politics, governments are free to adopt legislation with

[49] Cox, *Approaches to World Order*, 496.
[50] Walzer, *Just and Unjust Wars*, 106.
[51] J. L Holzgrefe and Robert O Keohane, *Humanitarian Intervention: Ethical, Legal, and Political Dilemmas* (Cambridge; New York: Cambridge University Press, 2003), 25.
[52] Holzgrefe and Keohane, *Humanitarian Intervention*, 38.

extremely weak, or even non-existent, implementation measures, states are free to create and accept international legal obligations that are to be implemented entirely through national action. And this is in fact what states have done with international human rights. None of the obligations to be found in multilateral human rights treaties may be coercively enforced by any external actor."[53] Historical examples from the last three decades alone of atrocities in Rwanda, Somalia, Darfur, Kosovo, Haiti, and elsewhere around the world suggest an agreeable threshold exists to satisfy *jus ad bellum* requirements of ethical intervention.

It is within this ethical framework that we must tackle the difficult questions we face regarding the justice *of* war and justice *in* war. While policy-makers decide whether a war itself is justified, individual soldiers must examine whom to kill and how to kill them.[54] These considerations have endured as long as warfare itself. While the character of war and the domains of warfare have changed, the nature of war and its ethical underpinnings have remained constant. Yet as we lead headlong into the wild frontier of cyberspace we must redress classical assertions of right and wrong. With the new capabilities proposed by the cyber domain come new responsibilities, fundamentally altered assumptions, a vacuum of norms, and ethical questions begging for answers. If we are to use this domain for acts of war we must carefully consider the ethical ramifications of our actions.

[53] As quoted in Holzgrefe and Keohane, *Humanitarian Intervention*, 44.
[54] Walzer, *Just and Unjust Wars*, 43.

Chapter 3

Ethics of Cyber Warfare

The previous chapter described a framework for ethical warfare. This chapter overlays the *jus ad bellum* and *jus en bello* standards that have come to define ethical warfare with unique considerations that cyberspace and cyber warfare bring to war. In some instances, the traditional just-war standards apply as neatly in cyberspace as they do in any other domain. In most, however, the nature of cyberspace and the capabilities the domain facilitates gives cause to rethink how we interpret our traditional mindset regarding ethics in war. Each facet presented in the foundational discussion of chapter 2 is broken out in detail below.

Good Faith

The ethical premise of good faith offers combatants in traditional wars assurances and options. Based largely on *prima-facie* obligations, the good faith imperative allows for ethical treatment of combatants when they are incapacitated or they choose to surrender. For example, wounded or sick combatants are guaranteed protection under the terms of the Geneva and Hague conventions.[1] The same conventions outline procedures and expectations for combatants who willingly surrender or who become prisoners of war.[2] These established expectations underwrite brutal combat with mutually accepted humanitarian norms.

Good faith between combatants plays a pivotal role in that it allows wars to end without one party obliterating the other. Enemy soldiers, citizens, or policy makers who expect brutal, treacherous treatment at the hands of their opponent are not likely to surrender. It is hard to imagine, for example, Emperor Hirohito accepting the allies' terms of surrender at the end of World War II if he believed allied forces would

[1] Michael Bothe, Karl Josef Partsch, and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff Publishers, 1982), 3.
[2] Bothe, Partsch, and Solf, *New Rules for Victims of Armed Conflicts*, 6.

ravage Japan anyway.[3] Good faith impacts both when and how wars are fought so it serves naturally important roles in both *jus ad bellum* and *jus en bello.*

One must reexamine several commonly accepted ideas of warfare in order to establish the groundwork for good faith in cyber warfare. First, fighters in cyberspace are often unnamed, unaffiliated, and difficult to pinpoint.[4] Second, specific attribution is difficult even in attacks that are carried out by identifiable sources.[5] Finally, time and space considerations change the ways in which fighters in cyberspace can be threatened or quelled. These considerations are particularly important when response options are limited to coercive physical threats. Incentives to surrender change entirely when they cannot be elicited by threatening belligerent parties. However, cyber warfare may also offer the military strategist legitimate, non-lethal ways to achieve desired ends. In this way, cyber warfare proposes novel methods by which to avoid treachery altogether. All of these complicated facets form a new understanding of good faith in the realm of cyberspace.

An apt place to start when examining the premise of good faith in cyber warfare is to identify the combatants. The term *combatant* traditionally describes a person who directly participates in warfare on behalf of a nation state, or someone who offers direct support to warring forces.[6] This distinction is important because combatants may be targeted legally under the Law of Armed Conflict.[7] However, the

[3] Tsuyoshi Hasegawa, *Racing the Enemy: Stalin, Truman, and the Surrender of Japan* (Harvard University Press, 2005), 215.
[4] Mejia, Eric F., Colonel, USAF, "Act and Actor Attribution in Cyberspace," *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 118.
[5] Mejia, Eric F., Colonel, USAF, "Act and Actor Attribution in Cyberspace," 119.
[6] The Judge Advocate General's Legal Center and School, MAJ William J. Johnson, and MAJ Andrew D. Gillman, *Law of Armed Conflict Deskbook: 2012* (CreateSpace Independent Publishing Platform, 2014), 74–75.
[7] Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," *Air Force Law Review* 64 (June 2009): 154.

definition of the term, and the circumstances surrounding its use, evolved as methods of warfare have changed.

The age of total war, coupled with the ability to strike deep within enemy territories, blurred the lines between combatants and non-combatants.[8] Deep strikes took wars to enemy territories that were previously immune to battlefield effects. In total wars, particularly the two World Wars, the citizenries of entire nations were mobilized in support of war efforts, giving some justification to the idea that the line between combatants and non-combatants no longer existed. In World War II, for example, aircraft factories and mechanical plants manned by civilian German citizens were considered legitimate military targets even though it would be a stretch to call the factory workers themselves combatants.[9]

The asymmetric conflicts of the 21st Century further complicated the ways in which combatants and non-combatants are differentiated. American rules of engagement in Afghanistan, for instance, labeled nearly anyone who demonstrated "hostile intent" a combatant.[10] This vague definition, coupled with strict limits on the acceptability of collateral damage, forced warfighters at the lowest tactical levels to decide what hostile intent looked like while bullets careened through the air. Or conversely, combatants in these irregular wars found themselves advantaged by the ambiguity between acceptable and unacceptable engagement.

If combatants in irregular warfare enjoy advantages of ambiguity, combatants in cyberspace are all but invisible.[11] General Wesley Clark

---

[8] Lester Nurick, "Distinction between Combatant and Noncombatant in the Law of War, The," *American Journal of International Law* 39 (1945): 680.

[9] R. J. Overy, *The Air War, 1939-1945*, 1st ed, Cornerstones of Military History (Washington, D.C: Potomac Books, Inc, 2005), 183.

[10] Kenneth Roth, "The Law of War in the War on Terror," *Foreign Affairs* 83, no. 1 (February 1, 2004): 4.

[11] Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36 (2011): 445; Mejia, Eric F., Colonel, USAF, "Act and Actor Attribution in Cyberspace," 121. Both Waxman and Mejia discuss the technical difficulty of attributing cyber-attacks to

and Peter Levin contend "There is no form of military combat more irregular than an electronic attack: it is extremely cheap, is very fast, can be carried out anonymously, and can disrupt or deny critical services precisely at the moment of maximum peril."[12] Warfighters in cyberspace may infect information systems years in advance of actual combat operations, leaving latent weapons capable of destroying or disrupting their targets. It is thought, for example, that the Stuxnet computer virus that damaged nuclear centrifuges in Iran's Natanz enrichment facility in 2010 may have been introduced into the systems clandestinely as early as 2005.[13]

Careto, an advanced cyber threat uncovered by Russia's Kaspersky Labs in February, 2014, serves as another telling example. Careto infiltrated computer systems in embassies and other government facilities within 30 Spanish speaking countries undetected since at least 2007.[14] Cyber warfighters can create cyber weapons that replicate themselves, morph to changing circumstances, or spawn subsequent infections autonomously while weapons lay in waiting. In these instances, the combatants who create and introduce weapons into enemy information systems in the first place have almost assuredly vanished back into the worldwide populous of non-combatants once hostilities commence.

---

specific sources. Even the most sophisticated independent actors, Internet security firms, and nations operating in cyberspace seldom find convincing evidence that links attacks to specific actors.

[12] Wesley Clark and Peter Levin, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses," *Foreign Affairs*, no. November/December 2009 (n.d.), http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway.

[13] Geoff McDonald et al., "Stuxnet 0.5: The Missing Link," *Symantec Security Response, February* 26 (2013): 2, http://www.symantec.com/ko/kr/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf.

[14] Donahue, Brian, "The Mask – Unveiling the World's Most Sophisticated APT Campaign," *Daily - English - Global - Blog.kaspersky.com*, accessed March 6, 2014, http://blog.kaspersky.com/the-mask-unveiling-the-worlds-most-sophisticated-apt-campaign/.

Active cyber warfighters engaged in real-time attacks are also extraordinarily difficult to identify and engage. Cyber warfighters may execute their craft at great distances from their targets. The worldwide nature of cyberspace makes it possible to initiate attacks from almost anywhere on the globe instantaneously.[15] Sophisticated adversaries are rarely able to navigate complicated labyrinths of information systems to follow cyber-attacks back to their specific electronic origins. The Internet and its larger cyberspace linkages are not designed in a way that favors positive identification and ownership.[16] Connecting elusive electronic signatures to physical locations and individual attackers is even more difficult. Even in the rare instances where exact physical origins of cyber-attacks are determined, the combatants who perpetuated the attacks seldom remain in physical proximity to the systems they used.[17] The combatants themselves are human beings but their operating environments and weapons are virtual, fleeting, and nebulous.

Nation states rightly find tremendous advantages in the anonymous and non-attributable nature of cyber warfare. By remaining anonymous, states retain the option to deny their actions in politically sensitive situations while achieving desired effects. Relatively weak nation states find themselves emboldened to attack stronger adversaries using cyber weapons when physical attacks would be politically or militarily untenable. The Syrian Electronic Army (SEA), for example, is a loosely affiliated group of programmers and activists within Syria that aims to counter potential American involvement in Syria's ongoing civil struggle. The SEA launched a wave of cyber-attacks against American interests in 2013-14 while hidden in the ambiguity of cyberspace. These attacks defaced numerous American information systems and even

[15] Derek S. Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012), 10.
[16] Erik M. Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem," *Air Force Law Review* 68 (January 2012): 179.
[17] Mejia, Eric F., Colonel, USAF, "Act and Actor Attribution in Cyberspace."

brought down the New York Times website for an entire day.[18] Physical attacks that produced the same level of destruction would have left attackers exposed to potential retaliation or physical harm. In cyberspace, however, the combatants maneuvered with impunity.

Anonymity and non-attribution in cyber warfare benefit strong nations as well. These factors allow nations responsible for creating and maintaining international norms to act outside existing ethical standards without fear of political backlash. For instance, cyber forensics experts traced numerous cyber-attacks launched against the republic of Georgia in 2008 back to information systems in Russia.[19] Lacking proof that specifically implicated the Russian government in the attacks, however, the international community was left without justification for retaliatory actions against Russia.[20] Additionally, anonymity and autonomy create military advantages in contested environments in the same way stealth technology, cruise missiles, and remotely piloted aircraft do. Nation states are incentivized to maintain capabilities to surprise and deceive their enemies in cyberspace in the same ways they are in the physical realms.

Anonymity and non-attribution, however, undermine the premise of good faith. Treaties, agreements, and norms – the basis upon which good faith rests – all depend on accountability and attribution. Treaties and norms are only viable forms of restraint for nation states that can be held accountable for their actions. When actions are attributable to legitimate actors on the global stage, the actors themselves have incentives to act ethically for fear of retribution or global condemnation.

---

[18] Mark Clayton, "In Any US-Syria Conflict, Cyberweapons Could Fly in Both Directions (+video)," *Christian Science Monitor*, September 6, 2013, http://www.csmonitor.com/USA/Military/2013/0906/In-any-US-Syria-conflict-cyberweapons-could-fly-in-both-directions-video.

[19] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, 2–3, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

[20] Noah Shachtman, "Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It | Danger Room | Wired.com," *Danger Room*, March 11, 2009, http://www.wired.com/dangerroom/2009/03/georgia-blames/.

Nuclear deterrence, for example, is built on the assumption that nuclear weapons have return addresses. Launching or dropping a nuclear weapon requires significant delivery capabilities, each of which has signatures that identify a weapon's source. Attribution and accountability go hand in hand to form the basis for ethical actions in war.

Given the sanctuary from which cyber combatants operate, where little fear of reprisal and even less fear of physical harm are routine expectations, one must consider whether incentives to surrender even apply. Soldiers in modern conventional wars surrender when they run out of physical or psychological options.[21] In Operation Desert Storm, for example, Iraqi forces surrendered by the thousands when they were encircled or when psychological operations forces were able to convince the Iraqis that they had no chance of success.[22] In cyberspace, however, enemies that are psychologically defeated still retain physical freedom of maneuver. Additionally, combatants in cyberspace retain the option to enter and exit the domain as they see fit.

The absence of practical ways to identify and locate attackers in cyberspace is troubling. The political and military incentives for nations to retain deniability are worrying. The ability to strike anywhere in cyberspace en masse or individually is unsettling. All of these factors combine to create a scenario where traditional terms of surrender and ethical treatment found in the Geneva and Hague Conventions are rendered nearly absurd. Combatants who face little fear of retribution should be expected to fight until their means or desires to do so are depleted. Therefore, the world is at a critical juncture with regard to the good faith premise in cyber warfare. While nations are incentivized in myriad ways to act subversively, these temptations erode stability. Norms of behavior established today will serve as the examples for the

[21] Daniel L. Haulman, *USAF Psychological Operations, 1990-2003*, May 23, 2003, 10.
[22] Gordon, *The Generals' War*, 347.

future.[23] These norms should favor, rather than undermine, peace. Actors in cyberspace should rely on *jus ad bellum* and *jus en bello* considerations for the altruistic merit these guidelines exhibit. Yet these same guidelines also create utilitarian advantages in that they establish standards that foster mutually-acceptable norms and a more predictable operating environment structured around acceptable and unacceptable limits.

Through a different lens, however, cyber warfare may actually help to redefine the good faith premise in a way that reduces violence in war.[24] Traditionally, weapons and tactics of war endure development cycles that forestall ethical judgment until after these new capabilities are fielded and used. Practices that are deemed treacherous, such as the employment of poisonous gasses and maiming land mines, are condemned by the international community and excluded from future wars. From the crossbow to nuclear intercontinental ballistic missiles, modern weapons trend toward increasingly lethality. While the world may never witness a full-blown cyber war, many of the capabilities that have emerged in this domain offer trustworthy methods to disarm combatants or negate defenses from great distances with less violence or treachery.[25]

Carl von Clausewitz famously established a framework of war that involves three inextricable components: primordial violence, policy, and chance.[26] Clausewitz surmises, "A theory that ignores any one of [these

---

[23] Stathis N. Kalyvas, *The Logic of Violence in Civil War*, Cambridge Studies in Comparative Politics (Cambridge ; New York: Cambridge University Press, 2006), 62. Kalyvas writes, "The norms that separate 'lawful' from 'unlawful' violence can be powerful…its origins lie in the medieval belief that war is permissible only if waged by legitimate authority…" While Kalyvas wrote primarily about civil wars and violence, his sentiment is quite valid with regard to the establishment of norms of behavior in cyber warfare.

[24] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, ed. Michael N. Schmitt (Cambridge ; New York: Cambridge University Press, 2013), 66, 180.

[25] David Fidler, *Inter arma silent leges Redux?*, in Reveron, *Cyberspace and National Security*, 73.

[26] Von Clausewitz, Howard, and Paret, *On War*, 89.

three elements] or seeks to fix an arbitrary relationship between them would conflict with reality to such an extent that for this reason alone it would be totally useless."[27] Yet cyber warfare tugs at the connection between violence and war. If, for example, a military becomes so reliant on information systems that it cannot execute a coordinated campaign without them, cyber weapons may be capable of rendering the military inert. A thorough examination of this facet is contained in the discussion on proportionality, but it is important to note the theoretical possibility that cyber weapons may reshape the good faith imperative by reducing scenarios in which treachery is even possible.

Many of the complicating factors surrounding cyber warfare and the good faith premise are exacerbated by the current state of technology available to cyber warfare practitioners. The medium of cyberspace and the practical technical capabilities of cyber warfare evolve so rapidly that technical methods of enforcing ethical standards in cyberspace are often defunct before they are fielded. If, for instance, technology matures in ways that make attribution of attacks easier, the good faith premise would be expected to apply to cyber warfare in ways understood more traditionally. The current state of technology, however, established rules and ethical norms must substitute for more technical methods of enforcement until technical capabilities mature.

Good faith, therefore, offers both troubling complications and intriguing opportunities to military strategists. When one wishes to achieve military effects anonymously, cyber warfare techniques may very well offer viable options. Conversely, however, when one wishes to identify an adversary, he may be frustrated by the very anonymity he enjoyed in different circumstances. Yet the incentives to operate in cyber warfare, including the ability to produce effects with less lethality than in other domains, makes cyberspace an operating environment that cannot

[27] Von Clausewitz, Howard, and Paret, *On War*, 89.

be discounted. Until technological safeguards and international laws governing cyber warfare emerge, however, norms of behavior are all that separate barbarism from professional conduct. These norms will help facilitate an environment where the good faith imperative applies.

Proportionality

Proportionality in war suggests combatants should use the minimum amount of force required to achieve legitimate objectives without causing undue harm or suffering.[28] Walzer refers to proportionality as "a matter of adjusting means to ends."[29] Strong connections between good faith and non-combatant immunity converge within the principle of proportionality. Combatants who measure means to coincide with legitimate ends, by virtue, adhere to many good faith principles. The same judicious practices limit harm to non-combatants to within ethically acceptable limits.

Both novel advances and nagging difficulties emerge when the principle of proportionality is transposed onto the tools and capabilities of cyber warfare. First, cyberspace is an inherently dual-use environment. Forces capable of planning and executing cyber warfare utilize the same transmission paths, systems, and software as peaceful participants in the cyber domain.[30] Next, the significant overlap with unpredictable commercial entities and civilians makes cyberspace a fluid environment. This unpredictability makes it difficult to measure the actual effects of cyber weapons against their anticipated effects.[31] Finally, this section will address possible ways in which cyber warfare potentially enhances the idea of proportionality by offering less lethal

[28] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 145.
[29] Walzer, *Just and Unjust Wars*, 120.
[30] Reveron, *Cyberspace and National Security*, 6.
[31] Edward Barrett, "Warfare in a New Domain: The Ethics of Military Cyber-Operations," *Journal of Military Ethics* 12, no. 1 (April 17, 2013): 10, doi:10.1080/15027570.2013.782633.

means to achieve desired ends. In theory, cyber weapons can be extraordinarily accurate in ways kinetic weapons cannot. Strategists, tacticians, and policy makers, however, must scrupulously examine the actual effects of their actions in cyberspace to ensure they abide by ethically acceptable standards of proportionality.

The distinction between military and non-military systems in cyberspace is much more convoluted than it is in the traditional realms of air, space, sea, and land. Tanks are able to lumber across land regardless of whether civilian roads are available. Air forces only require access to airfields in order to project power through the air. Naval vessels, in and of themselves, are often depicted as forward extensions of sovereignty and national power through the world's oceans. However, combatants engaged in cyber warfare are often completely reliant on commercial fiber optic cables, satellite links, airwaves, and traffic routing systems. The *2011 Department of Defense Strategy for Operating in Cyberspace* says "The challenges of cyberspace cross sectors, industries, and U.S. government departments and agencies; they extend across national boundaries and through multiple components of the global economy. In fact, cyberspace would not exist without the manmade backbone of electronic devices on which it functions.[32] Many of DoD's critical functions and operations rely on commercial assets, including Internet Service Providers (ISPs) and global supply chains, over which DoD has no direct authority to mitigate risk effectively."[33] Additionally, the actual systems used by combatants in cyberspace are usually supplied by commercial vendors in configurations that are widely available to the public. The United States, for example, codified the

[32] *Cyberspace and National Security*, 212.
[33] *Department of Defense Strategy for Operating in Cyberspace*, 8.

requirement to use commercial, off-the-shelf (COTS) technology where feasible in 1994 and this trend has continued for two decades.[34]

When cyber forces operate through commercial transport and computing systems, the cyber battlefield becomes an enmeshed tapestry of protected systems, viable targets, and neutral entities. In this way, cyber warfare encounters many of the challenges that have come to exemplify irregular warfare. In his book, *War from the Ground Up: Twenty-First Century War as Politics,* Emile Simpson writes "Today, even relatively conventional wars are not fought entirely within a sealed military domain. The means of war are not just combat."[35] Simpson carries this argument toward an important conclusion when he suggests "In terms of military jargon, one has to distinguish between 'means' and 'effects.'"[36] Warfighters in the traditional domains must balance how their actions affect their surroundings. Cyber warfighters, too, have a responsibility to understand how their actions impact the domain of cyberspace itself.

Viruses and botnets are two examples of weapons in cyberspace that can produce detrimental effects on the domain itself. Viruses spread between computers by infecting files within their host systems. Botnets are groups of compromised computers, often numbering in the millions, that are manipulated through command and control software to carry out collective acts of cyber warfare.[37] Both of these capabilities produce damaging side effects. Viruses destabilize all of the information systems they infect, regardless of whether the systems were targeted intentionally. Botnets often impede legitimate Internet traffic, degrade system access, and overflow network traffic management systems that

[34] William Perry, "Specifications and Standards - A New Way of Doing Business" (US Department of Defense Policy Memorandum, June 29, 1994).
[35] Emile Simpson, *War from the Ground up: Twenty-First Century Combat as Politics* (New York, NY: Oxford University Press, 2013), 69.
[36] Simpson, *War from the Ground up*, 72.
[37] Jason Andress, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Amsterdam ; Boston: Syngress/Elsevier, 2011), 203.

serve entities unrelated to the attacks. The collateral effects these cyber weapons produce are at the heart of the proportionality debate.

The United Nations International Telecommunications Union (ITU) champions the notion that Internet access promotes socio-economic growth and human prosperity. Efforts to promote broadband connectivity throughout impoverished areas of the world are underway with the stated goals of fairness, justice, and economic viability for all.[38] If the ITU is correct in its assessment that unobstructed connectivity should be treated as a basic human right, indiscriminate behavior in cyberspace can have the secondary effect of limiting this important source of development.[39] Failure to carefully limit collateral damage associated with cyber weapons can undermine peaceful and prosperous uses of the cyberspace domain. Cyber warfare strategists must measure the effects they aim to achieve versus the associated secondary costs when deciding whether proportionality is adequately addressed.

Secondary, unintended effects are not limited to the logical domain. Cyber weapons can also produce unintended physical effects. Attacks against Supervisory Control and Data Acquisition (SCADA) systems serve as a case in point. SCADA systems are designed to interface with industrial control systems to more efficiently manage pipeline systems, electrical grids, and several other civil support systems. SCADA systems rely on programmable logic controllers that are not unique to the systems they support.[40] Instead, these controllers support a variety of SCADA connections. Vulnerabilities that exist in electrical grids, therefore, may also be present in water pipelines and sewage

[38] H.E Kagame and Carlos Helu, *Transformative Solutions for 2015 and Beyond: Manifesto*, Broadband Commission for Digital Development (United Nations International Telecommunications Union), 6, accessed March 26, 2014, http://www.itu.int/net/broadband/Documents/working-groups/BBComm-ManifestoNames.pdf.

[39] "Broadband Commission for Digital Development Delivers Report - News," accessed April 24, 2014, https://itunews.itu.int/En/506-Broadband-Commission-for-Digital-Development-delivers-report.note.aspx.

[40] Andress, *Cyber Warfare*, 125–126.

management systems using similar programmable logic controllers. Justifiable attacks against military electricity sources, for example, can spread through a variety of methods to cause unintended damage in systems unrelated to the actual targets.

The ability to test and predict how cyber weapons will act when they are employed is another source of ethical contention. Edward Barrett of the Stockdale Center for Ethical Leadership at the US Naval Academy addressed this specific issue in an article titled *Warfare in the New Domain: The Ethics of Military Cyber Operations.* Barrett writes "Since well-tested, human-launched kinetic weapons operate within natural, stable, and relatively knowable conditions, their effects are predictable…But cyber-attack effects may be highly unpredictable due to their human-created and thus changing cyber-environment."[41] While some may see collateral damage of this nature as simply a cost of war, cyber warfare offers unique circumstances that have not been encountered in other forms of warfare. For example, Patrick Lin, Fritz Allhoff, and Neil Rowe opine "lack of control means an attack might not be able to be called off after the victim surrenders."[42] A virus propagating through cyberspace, or an autonomous worm traversing through networks pays little mind to peace treaties. Strategists must consider this facet of cyber warfare if these tools are to be used in war.

The examples above capture both *jus ad bellum* and *jus en bello* considerations that must be addressed in any ethical measurement of cyber warfare. Cyber weapons can potentially alter the very domain in which they operate in ways that cannot be tested. The very presence of these unknown effects, and the potential damage that may ensue, must be considered when deciding whether to employ cyber weapons. Stuxnet, one of the most sophisticated and specialized cyber weapons

[41] Barrett, "Warfare in a New Domain: The Ethics of Military Cyber-Operations," 10–11.
[42] Patrick Lin, Fritz Allhoff, and Neil Rowe, "Is It Possible to Wage a Just Cyberwar?," *The Atlantic*, June 2012, http://www.theatlantic.com/technology/print/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

known, for example, spread onto untargeted systems when humans inside the Iranian nuclear plant at Natanz inadvertently transferred the infectious code on portable data storage devices.[43] While Stuxnet caused little damage once it left Natanz, the next malicious code of this variety might bring substantial unanticipated effects. Meticulous care must be taken to examine the instances in which requirements for certainty outweigh the potential unknowns cyber weapons introduce. Tense political conflicts, for instance, require carefully calculated moves in order to avoid inadvertent escalation. Unanticipated cyber effects may be all that is required to tip the balance of control in a conflict of this sort.

One cannot assume that cyber warfare actions will be met strictly with in-kind responses. The United States National Military Strategy for Cyberspace Operations states "DOD will conduct kinetic missions to preserve freedom of action and strategic advantage in cyberspace."[44] One US Official is quoted, saying "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."[45] No instances of direct kinetic responses to cyber-attacks have been documented to date. However, it is no stretch to predict that as acts of cyber warfare increase in intensity, nations become more dependent on their cyber systems for normal state functions, and cyber warfare actions tend toward autonomy without humans directly tied to decision-cycles, escalation from the cyber domain to the physical realm is likely. If (or when) this type of response occurs, questions regarding proportionality will surface once again, asking if electronic attacks justify the potential loss of life associated with physical responses.

---

[43] McDonald et al., "Stuxnet 0.5."

[44] *U.S National Military Strategy for Cyberspace Operations*, 15.

[45] Siobhan Gorman And Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 31, 2011, sec. Tech, http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304563104576355623135782718.html.

The short description of proportionality at the beginning of this section highlighted two important characteristics. First, combatants should seek to accomplish their goals with minimal harm or suffering. The debate thus far has focused on that important clause. The second characteristic of proportionality, however, is the idea that combatants should use the minimum amount of force required to achieve objectives. Through this lens, cyber warfare turns from a potential *jus en bello* detractor to a highly capable supporter. Cyber weapons hold the potential to be tremendously precise and discriminate in ways kinetic weapons cannot.[46] Additionally, cyber weapons are often capable of achieving desired battlefield effects without the use of violence.[47]

Cyber warfare techniques offer strategists opportunities to achieve military objectives with unmatched precision. Some dual-use targets like power stations, for example, may be targeted in ways that only stop the flow of electrical current to circuits used by military equipment, leaving civilian energy supplies untouched. An additional advantage to this approach comes at the cessation of hostilities. Systems that are degraded or negated through cyber warfare are often not physically damaged. This introduces the possibility that systems can be turned back on rather than rebuilt. When this method is compared to contemporary techniques involving even the most precise kinetic weapons like precision guided bombs, obvious proportionality advantages emerge.

Limiting one's analysis to a simple comparison between cyber capabilities and existing weaponry, however, ignores novel ways in which cyber warfare can improve proportionality. Cyber weapons can simultaneously attack entire systems like command and control networks, financial enterprises, and military industrial schemes with paralyzing accuracy while producing very little physical collateral

[46] Randall Dipert, "Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy," *Journal of Military Ethics* 12, no. 1 (April 17, 2013): 38, doi:10.1080/15027570.2013.785126.
[47] Thomas Rid, *Cyber War Will Not Take Place* (Oxford ; New York: Oxford University Press, 2013), 170.

damage. Weapons prepositioned on these systems can await precise conditions, instructions, and leadership approval before they are put into effect. When designed properly, these weapons can be rendered inert remotely once hostilities cease. Unlike landmines, for example, that litter historical battlefields to this day, cyber weapons offer a more hygienic approach to warfare.

In certain instances, military advantages can be created through cyber warfare with only the presumption or threat of an attack. Low-level attacks that undermine trust in the fidelity or functionality of the targeted systems may lead decision-makers to resort to less effective alternatives. Therefore, a system may not need to be compromised at all as long as decision makers can be convinced that systems are compromised. As Thomas Rid states, "Cyber-attacks of all strands, even in their predominantly non-violent ways, may achieve a goal that previously required some form of political violence: to undermine the collective social trust in specific institutions, systems, organizations, or individuals."[48]

Yet strategists today must be careful to realize that the theoretical possibilities of cyber warfare remain outside the grasp of current technological capabilities. Cyber weapons today are rudimentary compared to the conceptual uses envisioned by experts in the field.[49] Theory regarding the capabilities of cyber warfare suggests a tendency toward near perfect precision. Precision implies a finely tuned gauge on proportionality. Policy makers who fail to appreciate this difference between theoretical and actual capabilities are apt to approve the employment of cyber weapons based on the promise of highly selective effects. In reality, the weapons at policy makers' disposal today may very

[48] Rid, *Cyber War Will Not Take Place*, 167.

[49] Antoine Bousquet, *The Scientific Way of Warfare.* (Columbia Univ Pr, 2010), 210. Several authors, to include many writers of science fiction, have created plausible scenarios involving future cyber weapons. Bousquet offers one example in his concept of swarming networks of sensors and electronic devices in the referenced work.

well cause unintended consequences as discussed earlier in this section. Additionally, these weapons may remain on the cyber battlefield as persistent threats for everyone operating in this realm.

Air power strategists faced a similar dilemma during World War II when precision bombing was touted as a method of attacking strategic vulnerabilities. This theoretical premise formed the basis of the allies' strategic bombing campaign against Germany. Actual aircraft capabilities, aircrew accuracy, and weapon precision, however, limited the efficacy of this strategy. Air power historian Michael Sherry, describing the US strategy of precision bombing writes "In a sense, the claim was technically correct, and [the] men really believed that because American planes still flew under directives assigning precise targets, nothing in American targeting practices had changed. But by the end of 1944, American bombers relied on radar or 'blind bombing' techniques so often…that terror became their inevitable consequence…"[50] Air power stood as a viable strategy when measured against its alternatives. Choosing air power, however, came at an ethical cost.

Just as air power matured to more accurately match its theoretical possibilities with its practical plausibility, so too must the weapons and practitioners of cyber warfare. A more granular understanding of cyber weapons, their anticipated and unanticipated effects, and the realm in which they operate is required if the ethical standard of proportionality is to be maintained. Therefore, policy makers face a proportionality dilemma. Cyber weapons today may achieve tremendous effects with little collateral damage at relatively low costs, but these weapons may produce unknown effects that are difficult to measure. Cyber weapons of the future will conceivably become more precise and measurable, but advances in these weapons require realistic testing. Until such time as technology can mature, policy makers must

[50] Michael S Sherry, *The Rise of American Air Power: The Creation of Armageddon* (New Haven: Yale University Press, 1987), 261.

choose whether the proportionality risks cyber warfare introduces are worth the effects it might possibly achieve.

Non-Combatant Immunity

Measured protection of civilians is a mainstay tenet of modern war. States and international institutions have protected civilians from harm through established regulations and norms ranging from merchant shipping protection under the law of the seas to astronaut protection under international space law.[51] Most just-war theorists argue from a position that at least minimizes harm to non-combatants in war. Walzer sums up the popular position, saying non-combatants are "men and women with rights and they cannot be used for some military purpose, even if it is a legitimate purpose."[52]

While non-combatant immunity is a widely accepted premise of war in the physical domains, very little has been written, and almost nothing has been codified into law that specifically protects non-combatants in cyberspace. Michael Schmitt and the other cyberspace experts who toiled for three years to create the *Tallinn Manual on the International Law Applicable to Cyber Warfare* coalesced on the notion that civilians should not be directly targeted with cyber-attacks.[53] But even the *Tallinn Manual's* interpretation of existing laws says a cyber-attack is an operation that "is reasonably expected to cause injury or death to persons or damage or destruction to objects."[54] By this definition, civilians are left vulnerable to many acts of cyber warfare that

[51] Leslie C. Green, *The Contemporary Law of Armed Conflict* (Manchester University Press, 1993), 161; Aldo Amando Cocca, "Advances in International Law through the Law of Outer Space, The," *Journal of Space Law* 9 (1981): 13.
[52] Walzer, *Just and Unjust Wars*, 137.
[53] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 113.
[54] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 106.

can be disruptive, even devastating, without causing physical damage or death.

Many plausible cyber-attack scenarios that experts predict are, in fact, aimed directly at civilian populations.[55] Richard Clarke, counter-terrorism and cybersecurity advisor to three US Presidents, leads a chorus of other influential thinkers who warn attacks against civilians are imminent. Clarke presents a compelling case that illustrates how malicious actors in cyberspace could target the electrical grids of cities, causing blackouts that could last for months.[56] He discusses how rudimentary attacks against industrial control systems that manage water treatment facilities and sewage management systems have already taken place. These attacks, if leveraged against key targets could affect non-combatants en masse.[57] The financial sector is another area that many experts predict will fall victim to massive cyber-attacks. Attacks against banking systems or stock exchanges that erase, confuse, or encrypt transaction data on a massive scale could grind national commerce to a standstill.[58] These types of attacks are more than proposed theoretical concepts; they have already taken place. The threat is prevalent enough that President Obama issued an executive order mandating improved cooperation between governmental agencies that protect against cyber threats and the commercial entities that control vulnerable critical infrastructure.[59]

The surface-level logical argument suggests non-combatants should be kept immune from cyber warfare in the same way they are

---

[55] Julie J. C. H. Ryan, *Leading Issues in Information Warfare and Security Research* (Academic Conferences Limited, 2011), 129.
[56] Richard A. Clarke, *Cyber War: The next Threat to National Security and What to Do about It*, 1st ed (New York: Ecco, 2010), 101.
[57] Clarke, *Cyber War*, 2010, 98.
[58] James F. Dunnigan, *The next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Citadel Press, 2002), 217; Clarke, *Cyber War*, 2010, 70.
[59] "Executive Order -- Improving Critical Infrastructure Cybersecurity | The White House," accessed April 6, 2014, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

protected from traditional warfare. This is especially true given the theoretical propositions that highlight cyber warfare's ability to be enormously selective.[60] If weapons *can* be highly discriminating, as the debate on proportionality suggests, they *should* be used in the most proportional way possible. However, this comparison assumes the effects of cyber weapons are comparable to those of traditional kinetic means of warfare. While many of the proposed uses of cyber warfare can by highly disruptive to civilians, most are either non-violent or only facilitate violence indirectly.[61] This is a critical point of difference between the ethics of cyber warfare and traditional just war ethical standards.

It is useful in this regard to think of cyber warfare in terms of Thomas Schelling's concepts of coercion. Schelling described the United States' nuclear weapons strategy of the late 1950s and early 1960s as one that directly targeted civilians. The reasons for this choice were twofold. First, nuclear war demonstrated the limits of total war where combat was no longer constrained to engagements between fielded military forces. Rather, entire countries and their civilians were targeted for annihilation.[62] Second, the coercive psychological effect of knowing one's populous was targeted for nuclear extinction was a powerful force in the decision-making processes of both sides of a potential nuclear exchange.[63] Schelling wrote, "We live in an era of dirty war."[64] Context, however, is critically important when comparing cyber warfare to nuclear warfare.

When violence is removed from the equation, or at least removed as it pertains to *nuclear* war, the concept of coercion takes new shape. Schelling writes "Military strategy can no longer be thought of, as it could

[60] Dipert, "Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy," 38.
[61] Rid, *Cyber War Will Not Take Place*, 25.
[62] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008), 23.
[63] Schelling, *Arms and Influence*, 22.
[64] Schelling, *Arms and Influence*, 27.

for some countries in some eras, as the science of military victory. It is now equally, if not more, the art of coercion, of intimidation, and deterrence."[65] Cyber warfare options that target electrical grids or financial systems may prove both coercive and non-violent. In the ethical decision-making hierarchy, where *prima-facie* duties take precedent, non-lethal cyber means of achieving desired effects may actually be preferred, even if they target civilians instead of military forces.

This counterintuitive strategy is reinforced by the possibility that cyber-attacks can be designed in ways that make them reversible.[66] Attacks on electrical grids, for example, seize control of key components rather than destroying the controls themselves. Attacks against financial centers can be designed in ways that encrypt key data, allowing attackers to maintain the logical keys that restore the systems to their previous state once demands are met.[67] This aspect of cyber warfare adds another layer of action to Schelling's lessons. Schelling's coercion and deterrence theories are what he calls "skillful *nonuse* of military forces."[68] It is conceivable in the scenarios mentioned above that coercion or deterrence may continue even after an actor launches cyber strikes.

Another dimension of non-combatant immunity that must be considered is whether states have the responsibility to protect their citizens from acts of cyber warfare. This is particularly poignant if scenarios exist where non-combatants can be targeted ethically as suggested above. Hobbes asserts the very reason states exist is to offer

[65] Schelling, *Arms and Influence*, 34.
[66] Reveron, *Cyberspace and National Security*, 39.
[67] R. Gandhi et al., "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *IEEE Technology and Society Magazine* 30, no. 1 (Spring 2011): 28–38, doi:10.1109/MTS.2011.940293.
[68] Thomas C Schelling, *The Strategy of Conflict* (Cambridge, Massachusetts: Harvard University, 1980), 9.

protection to their citizens.[69] Locke tempers Hobbes' staunch realism but still contends man surrenders obedience to a society in exchange for privileges and protection.[70] If cyber warfare is just another threat against a country and its citizens, it would stand to reason that a country would have the responsibility to protect its citizens from known cyber threats.

Vulnerabilities in cyberspace as they exist today, however, complicate the responsibilities of the state. Most commercial companies that produce cyberspace's hardware and software foundation operate internationally.[71] Therefore, vulnerabilities in these platforms are shared by all people who operate on similar systems, regardless of nationality. The companies that manage and maintain these systems are incentivized to fix vulnerabilities once they are discovered and made public in order to guarantee the image and integrity of their products. Yet actors who wish to operate offensively in cyberspace often rely on undiscovered vulnerabilities to gain access to target systems.[72]

This conundrum places states in a difficult dilemma. On one hand, states must protect their citizens. Citizens would be best protected if states acknowledge vulnerabilities when they are discovered so that domestic instances of these flaws can be corrected by the globally-based commercial entities that create and maintain cyber systems. On the other hand, however, states are tempted to preserve secret information about undetected vulnerabilities so that these system weaknesses can be

---

[69] Hobbes, *Leviathan*, 153. Hobbes writes "The end of Obedience is Protection; which, wheresoever a man seeth it, either in his own, or in anothers sword, ature applyeth his obedience to it, and his endeavor to maintaine it."

[70] John Locke, *Two Treatises of Government*, Student ed, Cambridge Texts in the History of Political Thought (Cambridge [England] ; New York: Cambridge University Press, 1988), 349.

[71] Companies like Alcatel-Lucent, Cisco Systems, Microsoft, Apple, and Google all operate on diverse, global bases of clients and infrastructure. Open source software platforms including all flavors of Unix and Wikipedia also operate far beyond the boundaries of any one nation. Most tout an international presence as a business and social strength.

[72] Matthew J. Sklerov, "Solving the Dilemma of Sate Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent," *Military Law Review* 201 (2009): 24.

used as access points for their own cyber weapons. Many actors in cyberspace actually pay substantial amounts of money for vulnerabilities known as *zero day exploits* that have been discovered but not yet corrected.[73] Actors in cyberspace, therefore, must decide whether the harm these vulnerabilities present to peaceful citizens is worth the price to ensure vulnerabilities are kept available for exploitation.

This scenario also highlights a source of conflict between commercial software and hardware companies, and the populations they service. If populations become dependent upon cyberspace for basic functions like banking, communication, and emergency services, a state's responsibility to protect cyberspace increases. As states find that more of their critical infrastructure like railway control systems, gas line valves, and electricity routing systems are connected to cyberspace, the responsibilities only increase further.[74] Commercial companies that are worried about maintaining adequate profit margins will compel states to assume as much of the responsibility for repairing vulnerabilities as they can.[75] This tension led President Obama to issue an executive order in February, 2013 detailing unprecedented cooperation and responsibility sharing relationships between commercial entities that manage cyberspace and the government agencies charged to protect people from cyber-attacks.[76] Powerful actors like the United States will increasingly find it necessary to cooperate with relatively lesser political actors and commercial entities in order to preserve order in cyberspace.[77]

Here again, however, the blurred line between combatants and non-combatants in cyberspace complicates efforts to draw ethical demarcation lines. Through cyberspace, civilians have another avenue

---

[73] Alan Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits," *Forbes*, accessed April 7, 2014, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.
[74] Joseph S Nye, *The Future of Power* (New York: PublicAffairs, 2011), 81.
[75] Nye, *The Future of Power*, 133.
[76] "Executive Order -- Improving Critical Infrastructure Cybersecurity | The White House."
[77] Nye, *The Future of Power*, 132.

they can use to support their states' war efforts with very little involvement in actual combat. Non-combatants who possess home computing resources, for instance, may allow their governments to leverage their systems for the cyber warfare activities of the state. Citizens may simply allow a voluntary form of botnet control software to be installed on their computers so that network bandwidth and computer processing power can be pooled for coordinated attacks. This approach is not without precedent. Russian computers launched attacks against websites in Estonia and Georgia in 2008 ahead of Russian military advances. A website called *StopGeorgia* provided a software utility dubbed *DoSHTTP* that allowed average citizens to choose target websites and click a button labeled "Start Flood." This action sent barrages of data toward targeted sites in coordinated denial of service attacks.[78]

Like the factory workers of World War II who produced aircraft and tanks to bolster war efforts, or citizens who purchased war bonds to fund military forces, citizens who augment cyber warfare activities share some responsibility for their actions. Should these *near-combatants* be considered somewhere on the spectrum between warring soldiers and peaceful, innocent civilians?[79] Walzer suggests counter-attacks against these cyber augmenters are only justified if the attackers present such a risk that they warrant action due to military necessity. This was the same verdict levied on the German U-boat crew that targeted the *Laconia*, a merchant vessel, in 1942.[80] Citizens engaged in cyber warfare, however, may be targeted with commensurate cyber weapons instead of physical responses. When violence is removed and effects are

[78] "Marching off to Cyberwar," *The Economist*, December 4, 2008, http://www.economist.com/node/12673385.

[79] Near-combatant is a term created by this author to describe a person who operates in the grey area between traditional understandings of combatants and non-combatants. While past conflicts have certainly entertained this notion as described in this text, cyberspace allows people to become passive participants in conflicts in ways physical domains do not. This changing context and associated capabilities requires new vocabulary that is still emerging in the dynamic field of cyber warfare.

[80] Walzer, *Just and Unjust Wars*, 148–149.

measured in damage to equipment and resources, the concept of military necessity takes new form. This topic will be explored further as it pertains to the ethical premise of *last resort.*

Non-combatant immunity seems as if it should be an uncompromising standard for warfighters. Yet the intricacies of cyber warfare create cause to question the fundamental aspects of ethical warfare as they exist today. Certainly, non-combatants should enjoy a measure of protection from harm, especially compared to their war-making counterparts. Where lethal options are all that remain against potential adversaries, however, one must consider whether non-lethal cyber strikes against civilians are more ethically justifiable. These decisions are further complicated as the threshold for citizens to engage themselves in state cyber warfare activities is continually lowered by technology. Cyber warfare not only changes the battlefield, it alters how, when, and where fighting occurs. These factors must be considered as strategists attempt to maintain an ethical advantage in cyberspace.

Last Resort

Michael Walzer concludes *Just and Unjust Wars* with a grim acknowledgement that man has yet to free himself from the trappings of war. Walzer writes "And yet [war] cannot be escaped, short of a universal order in which the existence of nations and peoples could never be threatened. There is every reason to work for such an order. The difficulty is that we sometimes have no choice but to fight for it."[81] The premise of *last resort* is the final arbiter of *jus ad bellum,* compelling potential combatants to wait until they have no choice but to resort to war. *Last resort* rests on the idea that fighting, as Walzer so eloquently described, should not occur until all other feasible options have been, argued, considered, and tried. Given the *prima-facie* responsibility to

[81] Walzer, *Just and Unjust Wars*, 327.

prioritize protection of life ahead of any type of conquest, it makes good ethical sense to reserve warfare until absolutely necessary.

Cyber warfare, however, does not easily wedge into the time-tested parameters of *last resort.* With *prima-facie* responsibilities as *last resort's* grounding principles, one must consider whether non-lethal actions in cyberspace break the threshold by which *last resort* is measured. Certainly, cyber-attacks that produce lethal effects, such as catastrophic flooding that could directly resort from an attack on a dam's control systems, should be treated just as any other act of warfare.[82] The *last resort* premise in cyber warfare aligns nicely when lives are threatened.[83] What about the larger portion of the theoretical cyber warfare spectrum that *does not* directly produce casualties? Should actions like those observed in the Stuxnet attack, for instance, be restrained in the same way as kinetic warfare? Should non-lethal attacks even be considered acts of war? These are the questions the remainder of this section will address.

The Tallinn Manual intentionally creates distinction between the terms *cyber-attack* and *cyber operations.* Cyber operations, the manual says, describe "The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace."[84] A cyber-attack is a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[85] The members of Tallinn's International Group of Experts agreed that cyber operations that do not rise to the level of

[82] "Sensitive Army Database of U.S. Dams Compromised; Chinese Hackers Suspected," *The Washington Times*, accessed April 9, 2014, http://www.washingtontimes.com/news/2013/may/1/sensitive-army-database-us-dams-compromised-chines/.

[83] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge ; New York: Cambridge University Press, 2013), 43.

[84] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 258.

[85] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 106.

cyber-attacks should still comply with international laws, including the law of armed conflict.[86]

This distinction draws out the important idea that cyber warfare, defined in this study as actions by state or non-state actors that exploit an adversary's information systems in order to further political objectives, can be either lethal or non-lethal. Additionally, some non-lethal cyber operations can produce effects similar to those of kinetic strikes without causing permanent damage.[87] A strategist who approaches cyber warfare looking for a clear delineation between peace and war in the traditional sense will certainly be disappointed.

The *last resort* in cyber warfare cannot be addressed in an abstract set of rules or tripwires. Each instance and decision where cyber warfare may be justifiably employed depends heavily on its context.[88] Instead, it is helpful to place the range of cyber operations that can be used as acts of cyber warfare on a spectrum along traditional *jus ad bellum* and *cassus belli* considerations.[89] See figure 1 below.[90] Relative peace, where any act of war would be deemed aggressive in nature, lies on one end of the spectrum. On the other is total war, where ethical considerations are secondary to existential threats. When disagreements arise, international norms and laws establish guiding principles for the use of enforcement mechanisms short of war. Conflicts that escalate to untenable levels are examined within existing international legal and ethical frameworks before the use of force is authorized. Generally

[86] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 43.
[87] Rid, *Cyber War Will Not Take Place*, 34.
[88] Edward T. Barrett, "WARFARE IN A NEW DOMAIN: THE ETHICS OF MILITARY CYBER-OPERATIONS," *Journal of Military Ethics* 12, no. 1 (April 2013): 6, doi:10.1080/15027570.2013.782633.
[89] Rid, *Cyber War Will Not Take Place*, 9. Rid developed the idea of a spectrum for cyber offenses. Rid's spectrum stretched from "ordinary crime all the way up to conventional war." This work builds on Rid's concept, but does so with a different end objective in mind.
[90] Figure 1 was created by this author to clarify the way in which cyber capabilities potentially lower the threshold for acceptable preemptive, preventative, and putative actions

speaking, this process occurs under Articles 42 and 51 of the United Nations Security Council. These articles permit the use of force when

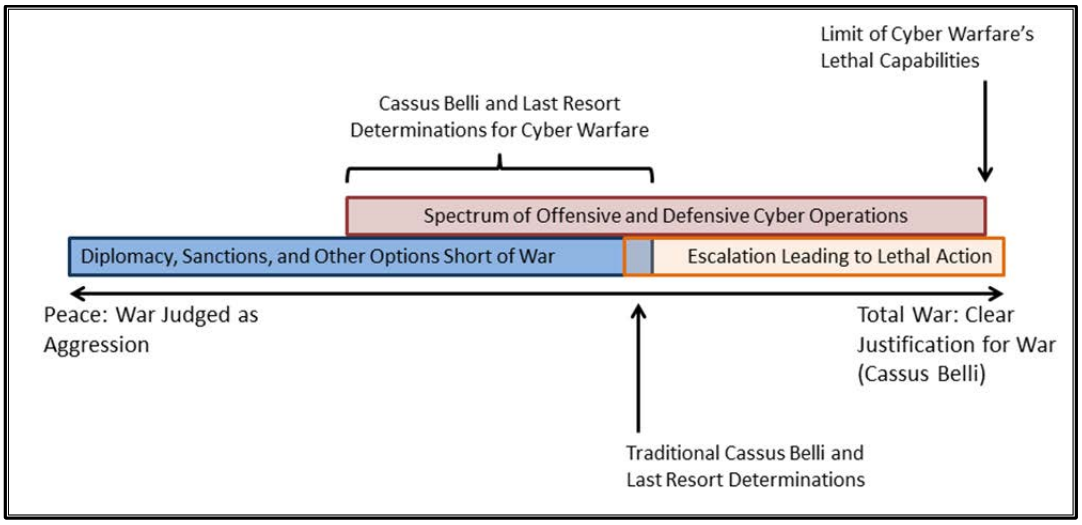

Figure 1: Spectrum of Conflict and Cassus Belli (Author's original work)

the Security Council votes to authorize such activity or when states must fight in self-defense.[91] Cyber warfare, however, overlaps existing options that change a conflict's decision calculus. Non-lethal cyber warfare options may conceivably be justified before more traditional forms of war if they help de-escalate a conflict or negate threats from aggressive adversaries.[92] As conflicts tilt further toward war, some cyber warfare scenarios, particularly those deemed cyber-attacks by the Tallinn Manual definition, may be met with more traditional, lethal responses.[93] Relatively small harassing attacks may also accumulate to damaging levels that justify kinetic or cyber retaliation.[94] David Gewirtz, an international cyber security and antiterrorism expert, illustrated this

[91] Mejia, Eric F., Colonel, USAF, "Act and Actor Attribution in Cyberspace," 115.
[92] Randall R. Dipert, "OTHER-THAN-INTERNET (OTI) CYBERWARFARE: CHALLENGES FOR ETHICS, LAW, AND POLICY," *Journal of Military Ethics* 12, no. 1 (April 2013): 37, doi:10.1080/15027570.2013.785126.
[93] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 106.
[94] Barrett, "WARFARE IN A NEW DOMAIN," 6; George R. Lucas Jr, "Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets," in *Presentation at Society of Philosophy and Technology Conference, University of North Texas*, 2011, 5, http://www.elac.ox.ac.uk/downloads/Permissible%20Preventive%20Cyberwar%20UNESCO%202011.pdf.

concept through the example of industrial attacks. Gerwirtz said, "When there are constant, advanced, persistent attacks targeting America's energy grid, and when some of them make it through to the point of keeping at least one power plant offline for weeks, that's no longer just cyberwar, that's war."[95]

A fundamental assumption in this discussion is that attribution can be established. A known difficulty in cyberspace discussed earlier, attribution is essential to any justified response. Without clear evidence that identifies the perpetrator of an attack or imminent threat, one may inadvertently target the wrong party.[96] When attacks can be directly attributed to a state, justified responses are easier to create and endorse. When cyber warfare actions emanate from *within* a state, but no clear ties to government can be established, response actions not only must assume attribution, they must assume states are responsible for the actions of their citizens.[97] While these are fundamental aspects of ethical warfare, they are particularly poignant in cyberspace where anonymity is simple to achieve, and innocent parties are often wrongfully implicated.[98]

With this framework in mind, the focus turns to a more refined examination of offensive and defensive actions that fall within the *last resort* grey area cyber warfare creates. Offensive actions that produce cyber effects without causing physical damage or loss of life, for instance, may be acceptable under existing international law.[99] Microsoft's Active Response for Security, dubbed *Project MARS*, serves as a case in point. According to Microsoft, *Project MARS* "is focused on combining legal and

---

[95] David Gewirtz for ZdNet Government | February 5 and 2013-- 17:42 Gmt, "Is Preemptive Cyberwarfare Good National Security Policy?," *ZDNet*, accessed April 10, 2014, http://www.zdnet.com/is-preemptive-cyberwarfare-good-national-security-policy-7000010857/.

[96] Martin C Libicki and Project Air Force (U.S.), *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 61, http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=304894.

[97] Mejia, Eric F., Colonel, USAF, "Act and Actor Attribution in Cyberspace," 118.

[98] Barrett, "WARFARE IN A NEW DOMAIN," 8.

[99] Maj Gen Charles J. Dunlap Jr, "Some Reflections on the Intersection of Law and Ethics in Cyber War," *Air & Space Power Journal* 27 (2013): 24.

technical acumen to proactively disrupt criminal infrastructure. This includes taking down botnets…seizing the infrastructure and domains criminals use to control them and taking the information we gain in those efforts to help better protect the Internet community and our customers."[100] This effort is geared primarily toward protection against economic threats but the same concept could apply to anticipatory state efforts against threats below the threshold for cyber-attacks. While these actions may appear offensive, their goal is one of defense and protection against ongoing, persistent, detrimental cyber operations.

Offensive cyber warfare actions outside the legal framework for *cassus belli* are likely to be judged based on estimates of the opposing threat's severity and imminence. Much like the case for preventative or preemptive actions in a more traditional sense, the onus is on the perpetrator of offensive cyber warfare actions to prove offensive actions were justified. Some experts argue that the unique capabilities cyber warfare introduces may allow conflicts to be diffused before they rise to the level of war.[101] Stuxnet, for example, is credited with at least delaying war between Iran and its adversaries by setting back Iran's nuclear enrichment program.[102] However, others will argue that small-scale offensive cyber actions can quickly escalate in unforeseen ways that actually lead more quickly to war.[103] Still others will argue that small planning and preparatory incursions into adversary weapons systems are necessary in order to prepare the cyber-battlefield for possible conflicts. While opponents would view these activities as

[100] "Malicious Software Crimes," accessed April 10, 2014, http://www.microsoft.com/government/ww/safety-defense/initiatives/Pages/dcu-economic-crime.aspx.
[101] Rid, *Cyber War Will Not Take Place*, viii.
[102] Rid, *Cyber War Will Not Take Place*, 32–34.
[103] Dipert, "OTHER-THAN-INTERNET (OTI) CYBERWARFARE," 36; Libicki and Project Air Force (U.S.), *Cyberdeterrence and Cyberwar*, 63.

unnecessary and unethical subversion, proponents view these preemptive steps as prudent planning.[104]

While the fundamental motivations and processes behind the *last resort* premise remain sound when applied to cyber warfare, implementation of these concepts requires intellectual, political, and technical savvy. Aggressive action is universally bemoaned by scholars of ethics in cyberspace as it is in any other medium. That said, the distinction between aggression, active defense, and meticulous preparation is blurred by the spectrum of effective lethal and non-lethal activities cyber warfare introduces. The *last resort* premise is still vital to the sanctity of *prima-facie* responsibilities, but instances exist, whether they are deemed war or some action short of war, where cyber warfare techniques may be judiciously employed before other more traditional forms of war.

Sovereignty

One final concept that deserves a fresh look in this examination of cyberspace and cyber warfare is sovereignty. Cyberspace continues to rapidly expand around the globe in new and unexpected ways. Transoceanic cables connect the world's land masses, allowing enormous amounts of data to transit between connected nodes literally at the speed of light with little regard for physical distances or borders[105]. Satellites in orbit allow anyone with a credit card and an antenna to establish private, unregulated connections to cyberspace regardless of where they are on Earth.[106] To illustrate how cyberspace has changed the world,

[104] David E. Graham, "Cyber Threats and the Law of War," *Journal of National Security Law & Policy* 4 (2010): 10.

[105] How-to Geek, *Interactive Cable Map Showcases High Speed Undersea Cables Around the World,* accessed 7 Jun 2014, http://www.howtogeek.com/95711/interactive-cable-map-showcases-high-speed-undersea-cables-around-the-world/

[106] Miniature, personal satellites antennas are common in many remote regions. While equipment and service costs are barriers to many, the technology is maturing and prices are falling. For one example of

imagine an American citizen boarding a plane bound for Seoul, South Korea with no passport or other documentation other than his name and place of origin. When he arrives in Korea he transitions to a waiting helicopter that flies to a shop in Beijing, China and lands. The man then enters the shop, buys a toy for his child using American dollars, and returns to the United States via the same route. As we know, this type of transaction occurs millions of times every day in the global marketplace facilitated by cyberspace without the complexities of distance or international borders. Even if the countries involved were to acquiesce and allow these types of legitimate, yet intervening, transactions to occur in the physical world as they do in cyberspace, we must accept the fact that acts of cyber warfare occur with the same disregard for established borders.[107]

Some countries have been marginally successful at limiting the types and sources of content that enter and exit their physical borders via cyberspace through the use of carefully engineered networks. China's "great firewall" is the most well-known example of such a configuration. All known connections to the global Internet are filtered at China's borders to cyberspace. Many of the world's most visited websites are blocked or substituted with alternatives that are approved by the Chinese government.[108] However, influential commercial entities like Google have shown some leverage in convincing oppressive governments to relax their filtering practices in exchange for their business.[109] Users have also found ways to circumvent even the most advanced filtering systems through the use of sophisticated anonymity and encryption

---

methods that can be used to access the Internet from anywhere on earth, see http://www.groundcontrol.com/one-touch-flyaway_001.htm

[107] On May 1, 2013 multiple sources in the U.S. media reported that actors in China carried out cyber-attacks targeting the US Army Corps of Engineers' databases containing sensitive details about America's hydro-electric damns. See http://freebeacon.com/the-cyber-dam-breaks/ for one example of a report.

[108] See www.greatfirewallofchina.org for an interactive search of websites and resources that are blocked in China

[109] Rebecca MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom (New York: Basic Books, 2012), 36-37.

tools.[110] The Internet was not built with international borders in mind and almost all attempts to mold cyberspace into adherence with existing physical boundaries have resulted in porous cyber-borders at best. When combined with the speed and relative anonymity inherent in movements through cyberspace, sovereignty becomes a concept of very little consequence and one that is even less enforceable in the cyber realm.

The core concepts of Westphalian sovereignty, however, still form the foundation of international relations. While it is helpful to consider cyberspace as a unique domain, one should caution against the temptation to treat cyberspace in isolation from other existing power structures. The array of electronic devices that form the structure of the domain can be changed and manipulated to fit existing international structures. While many nations and international institutions, including the United States, have become increasingly dependent upon cyberspace for government, economic, and military functions, the domain itself continues to expand globally. The very strategies nations create to govern, expand, utilize, and deny cyberspace to others actually shape the domain. This scenario presents an ironic connection between cyberspace and the physical world. The cyberspace environment allows people to connect in ways that were previously impossible. This tends to erode the importance of international borders and state power. At the same time, however, the way states approach cyberspace actual influences the strength and reach of the domain itself.

The aforementioned scenario creates tension between cyberspace and existing power structures. Some leaders view cyberspace as a welcome force for openness and prosperity, as in the case of the ITU's

[110] The Wall Street Journal: "No VPN? No Problem. A New Way Around China's Great Firewall," November, 2012. http://blogs.wsj.com/chinarealtime/2012/11/29/no-vpn-no-problem-a-new-way-around-chinas-great-firewall/

push to expand broadband connectivity for global prosperity.[111] Others, however, see cyberspace as a threat that undermines legitimate forms of government, as the recent case of the Turkish Prime Minister's ban on YouTube and Twitter demonstrates.[112] This tension makes cyberspace a dynamic environment. As virtual services, capabilities, and connections ebb and flow based on governmental policies they reshape the map of cyberspace. All the while, however, the physical map which contains national borders and traditional understanding of sovereignty serves as a guiding baseline for cyberspace's development.

The question becomes one of state *responsibilities* for cyberspace. Is a state responsible for the legitimate and illegitimate actions that originate from within a state's borders? At first pass, it seems logical to levy this duty on states in the same way nations are accountable for anything else that emanates from their borders. Aircraft that leave one state to bomb another are certainly the responsibility of the originating location. Even radio waves that start in one state and affect the spectrum in another nation must be controlled by their originators.[113] The Tallinn Manual suggests states are not only responsible for the systems, cables, and routing systems inside their borders, they are also responsible for their assets held in international waters and in space.[114]

On the other side of the argument, however, one finds equally convincing evidence suggesting states' responsibilities for their physical and virtual corners of cyberspace only go so far. The attribution problem discussed at length in other sections of this essay makes it difficult for states to conclusively pinpoint sources of threatening cyber activity emanating from within their borders. Additionally, the distributed

---

[111] Kagame and Helu, *Transformative Solutions for 2015 and Beyond: Manifesto*.
[112] "Turkey Blocks YouTube as Audio of High-Level Meeting on Syria Leaks," *The Lede*, accessed April 11, 2014, http://thelede.blogs.nytimes.com/2014/03/27/turkey-follows-twitter-ban-with-block-on-youtube-as-audio-of-high-level-meeting-on-syria-leaks/.
[113] ITU-R, "Rules of Procedure," *ITU*, accessed April 11, 2014, https://www.itu.int/pub/R-REG-ROP-2012.
[114] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 23, 26.

architecture of cyberspace control, where no one nation retains the ability to shape the environment in its entirety, leaves states with only limited capabilities to hinder some types of activities should they decide to do so.[115] The cyberspace is so vast and ever-changing that the most technically-proficient nations cannot feasibly be expected to defend against or limit the plethora of threats that exist.[116] Therefore, it is difficult to hold states accountable for something they cannot control.

The complicated relationship between commercial entities and governments further complicates the sovereignty debate in cyberspace. The United States government, for example, has found itself reliant upon commercial cyberspace service providers and critical infrastructure systems. This reliance is so strong that normal societal functions like utility services and transportation management could be severely impacted if the commercial systems cease to operate as they should. Nations now must decide how much authority they have to impinge on the commercial viability and profitability of these providers by forcing them to implement expensive security and functionality safeguards. The United States is working through this exact scenario now. President Obama's Cyberspace February, 2013 Executive Order detailing requirements for critical infrastructure protection serves as case in point.[117]

When threats emanate from within a nation's borders and the government of that nation is hampered by the limitations noted above, one must consider whether third parties – other nations, commercial entities, and non-state actors – have the right to intervene to quell threats. Certainly, all of the *jus ad bellum* and *jus en bello* considerations addressed thus far would still apply. If these criteria are met, however,

[115] Kim G. Von Arx and Gregory R. Hagen, "Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control," *Rich. JL & Tech.* 9 (2002): 4–8.
[116] Brent Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Forces Quarterly*, no. 61 (Quarter 2011): 10–17.
[117] "Executive Order -- Improving Critical Infrastructure Cybersecurity | The White House."

the question remains whether a nation has the right to do as Microsoft has done with Project MARS in terms of sovereignty.[118] In the more traditional definition of sovereignty, the entire notion of ethical intervention suggests nations are only entitled to the benefits their borders provide so long as they are capable of managing their domestic affairs.[119] One could certainly imagine scenarios where a nation would decide to virtually intervene to stymie cyber threats or cyber-attacks from within another nation's borders.

Culmination

The ethical considerations explored here are only a subset of those facing national decision-makers, security practitioners, and strategists at all levels. The world is watching. As powerful actors continue to move more effort toward cyberspace and the capabilities facilitated through this domain, norms of behavior will continue to develop. The United States is in a unique position of both great power and great vulnerability in cyberspace. American ability to project power in cyberspace is tempered to a great degree by corresponding vulnerabilities. With technological and physical safeguards against these weaknesses mired in political and technical difficulties, norms of acceptable behavior become defacto defense. US Secretary of Defense, Chuck Hagel, presented a speech at the headquarters of United States Cyber Command in March, 2014 in which he said the United States would "maintain an approach of restraint to any cyber operations outside of U.S. government networks." Hagel added, "We are urging other nations to do the same."[120] As the world struggles to develop appropriate guidelines for cyberspace and

[118] Microsoft, "Malicious Software Crimes," *Microsoft in Public Safety & National Security*, accessed April 10, 2014, http://www.microsoft.com/government/ww/safety-defense/initiatives/Pages/dcu-economic-crime.aspx.
[119] Holzgrefe and Keohane, *Humanitarian Intervention*, 25.
[120] Helene Cooper, "Hagel Seeks Peace Pact for Digital Realm," *The New York Times*, March 28, 2014, http://www.nytimes.com/2014/03/29/us/politics/hagel-seeks-peace-pact-for-the-digital-realm.html.

cyber warfare, these words must be matched with actions that build on ethical framework this document moves forward.

Chapter 4

Theory, Strategy, and Reality

Technology helps change civilizations. New innovations are grafted into societies by innovators who tout improvement and advancement. The same advances that make life easier, faster, clearer, and simpler, however, often have military utility, ushering in commensurate changes in the ways people fight wars. Cyberspace most certainly fits this dual-edged description. Global harmony and synchronization are made possible by the light-speed communication and collaboration capabilities cyberspace provides. Simultaneously, however, cyberspace offers the ability to put crosshairs on previously-immune targets in novel ways through cyber warfare. As these capabilities emerge, responsible actors will not simply ask if an action *can be done*; they will ask if it *should be done.* The arguments presented in the first three chapters of this paper confront some of the questions at the heart of this ethical debate.

This chapter presents a hypothetical scenario that builds upon actual tension that exists in the world today. In 1930, as air power was coming into its own as a force for good and a force for war, Giulio Douhet undertook a similar exercise in his essay, *The War of 19--.*[1] Douhet was solicited by Rivista Aeronautica to contemplate how the emerging capabilities of air power would weave into future wars. His thoughts on this challenge resonate with the task at hand:

> I have to confess that the invitation extended to me by the editor of this review greatly pleased me, and I accepted it at once, but perhaps thoughtlessly, as I realized as soon as I began to consider the task I had undertaken.
>
> The subject was to be a description of a hypothetical conflict among the great powers in the near future. A difficult subject in any case, and more so when I considered that it was not

[1] Giulio Douhet, *The Command of the Air*, Fire Ant Books (Tuscaloosa, AL: University of Alabama Press, 1998), 299–394.

> a question of idle imaginings or flights of fancy. Rather, I must submit to the tight rein of logic and the strait jacket of reason, since I was to write a serious work for a reputable military review, and I had to achieve the practical end of teaching something to the present by means of imagined happenings in the near future. If I had not given the editor my formal acceptance, and, what was worse, if the review had not published an announcement of the forthcoming work, I should gladly have given up the task. But there was no way out, and I had to go on.[2]

While Douhet's prophesy was ultimately judged by many to be an overly fervent prediction of air power's decisiveness in war, his words describing the challenge of technological prediction are prescient. This work does not portend to be as masterful as Douhet's, nor will it be as zealous. It will, however, undertake a similar challenge by attempting to bring to life the ethical considerations of cyber warfare before this discipline has matured fully.

The Korean Armistice: Cyber Warfare and a Modern Standoff

It is the year 2015 and tension continues to build on the Korean peninsula. In the north, the Democratic People's Republic of Korea (DPRK) continues to strengthen its nuclear weapons program and rattle the sabres of war. The rhetoric and aggressive actions of the DPRK leave the southern Republic of Korea (ROK) and many of its international partners feeling increasingly threatened and vulnerable.[3] Conventional forces and missile systems are amassed on both sides of the 38th parallel while international political and diplomatic powers attempt to control the potential crisis.

The DPRK's Supreme Leader, Kim Jong-un, celebrating his country's increasing military prowess, announced that he will proceed with another nuclear weapons test to demonstrate his country's expanding global influence. Fears swirl that this test could combine the DPRK's modernized medium range ballistic missile program with its

[2] Douhet, *The Command of the Air*, 294.
[3] Paul B. Stares, "Military Escalation in Korea," *Council on Foreign Relations, Center for Preventive Action*, 2010, 1, http://i.cfr.org/content/publications/attachments/CPA_contingencymemo_10.pdf.

miniaturized nuclear warheads in North Korea's first-ever nuclear launch beyond the confines of its own borders.[4] Japanese and American Aegis cruisers are positioned to shoot down any missiles that threaten South Korea, Japan, or any other nations within range of the anticipated missile test.[5] Additionally, other more creative steps have been taken behind the scenes to hedge against a successful missile launch.

Unbeknownst to the North Korean government, portions of their medium range missile launch and tracking system have been compromised clandestinely through the use of a sophisticated malware program. The program, code named Operation PANDORA, is able to interrupt the missile firing sequence in a handful of ways that appear to be normal mechanical failures.[6] The code was inserted remotely and is awaiting further commands from its creators. The main objective of Operation PANDORA is to undermine the confidence DPRK military operators and decision-makers place in the missile systems so that they choose to delay further tests -- especially tests with live nuclear munitions.

The creators of the code used in Operation PANDORA have not been disclosed, but secondary indicators suggest the source code was emplaced in a joint venture between South Korea and a trusted partner. The operators who installed the malware spared no expense to ensure anonymity for all parties involved. If successful, this effort will stall several potential missile tests on the launch pad before they are able to stir international fervor, elicit escalatory responses from threatened

---

[4] "Fact Sheet: North Korea's Nuclear and Ballistic Missile Programs," *Center for Arms Control*, accessed April 14, 2014, http://armscontrolcenter.org/publications/factsheets/fact_sheet_north_korea_nuclear_and_missile_programs/. It is conceivable that North Korea will overcome technological hurdles that currently prevent it from marrying its missile and nuclear weapon programs.

[5] Angela Erika Kubo, Jake Adelstein, "Japan Prepares to Shoot North Korean Missiles Out of the Sky," *The Daily Beast*, April 10, 2014, http://www.thedailybeast.com/articles/2014/04/10/japan-prepares-to-shoot-north-korean-missiles-out-of-the-sky.html.

[6] "S. Korea Seeks Cyber Weapons to Target North Korea's Nukes," *The Diplomat*, accessed April 14, 2014, http://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/.

nations, or cause unintended catastrophe should a dangerous missile fly off course.

Simultaneous to the increased rhetoric regarding nuclear systems, the North Korean government has expanded its foray into the realm of cyber warfare. After launching a series of attacks against South Korea in 2013, the DPRK has added thousands of "cyber-warriors" to its cyber operations units. Presumably, these units now have more advanced options capable of paralyzing financial systems, utility services including water and electrical supplies, and command and control systems within various targeted countries.[7] This development complicates Operation PANDORA because it offers North Korea heightened cyber expertise and more in-kind responses should the DPRK discover the malware operating on their systems.

Operation PANDORA appears on the surface to be an extraordinarily attractive option for policy makers who wish to limit North Korean antagonism while extending the timeline for more peaceful options to succeed. This operation falls below the internationally accepted threshold of a cyber-*attack* because it does not cause physical damage to the systems it targets.[8] Furthermore, the operation is designed to mimic mechanical malfunctions so that it does not resemble an escalatory move at all. While North Korean motives may remain unchanged as Operation PANDORA unfolds, this non-lethal, relatively unobtrusive, computer code may help de-escalate the impending crisis. The cyber operation is highly precise, creating almost no collateral damage in its wake. This level of discrimination also creates unmatched proportionality when measured against other options that stand a reasonable chance of success.

---

[7] "North Korean Cyber-Rattling," *The Economist*, May 17, 2013, http://www.economist.com/blogs/babbage/2013/05/digital-warfare.

[8] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013, 106.

The arguments articulated in the preceding chapters of this paper, however, should prompt a closer examination of Operation PANDORA before one is swayed to offer endorsement. In particular, three key assumptions Operation PANDORA takes for granted warrant a more detailed look. First, one should consider whether the code used in Operation PANDORA will behave as expected. Unintended side-effects could undermine the foundation of precision and proportionality that make this option so attractive in the first place. Next, one should look past intended effects and perceived anonymity to determine if the existing threat warrants a preventative or preemptive act. What one party perceives to be a desperate preemptive move may be interpreted elsewhere as unjustified aggression. Finally, one should consider how this type of subversive act shapes internationally-accepted norms in cyberspace.

If recent examples from 2012 to 2014 offer any indication, the code used in Operation PANDORA may potentially spread. The Stuxnet program, for instance, spread rapidly when it was unintentionally transferred outside its target network.[9] The Shamoon virus, a politically motivated attack against the Aramco refinery in Saudi Arabia, erased data on more than 30,000 computers. The virus also spread to refineries in other countries through methods the attack's originators never expected.[10] These precedents demonstrate how difficult it is to test sophisticated malware against conditions the program will encounter in the live environment of cyberspace. Even when machines act in highly predictable ways, humans interacting with machines may spread code from Operation PANDORA in ways that cause further instability or harm. The creators cannot predict confidently the effect Operation PANDORA

[9] McDonald et al., "Stuxnet 0.5."

[10] Christopher Bronk and Eneken Tikk-Ringas, "Hack or Attack? Shamoon and the Evolution of Cyber Conflict," *Survival, Global Politics and Strategy*, no. March 2013 (February 1, 2013): 3, http://bakerinstitute.org/files/641/.

will have on non-combatants or the medium of cyberspace itself if the code propagates in unintended ways.

Even if Operation PANDORA achieves its desired effects with the level of precision its creators anticipate, political leaders must objectively decide whether the existing threat warrants this type of aggressive action. Walzer reminds us that the burden of proof in any preemptive or preventative engagement rests with the aggressive actor.[11] The proctors of Operation PANDORA must consider whether an incursion into sovereign North Korean territory, whether physical or virtual, is justified given the fact that the DPRK publicized its upcoming launch as a test. A non-lethal invasion of sovereignty is an invasion nonetheless.

While Operation PANDORA is designed to help deescalate the existing crisis, the planners responsible for this event must appreciate the lack of international treaties, laws, and norms governing this type of activity. The operation is designed to be non-lethal and non-destructive. If the North Korean government interprets this incursion as an act of war, however, they are likely to respond in an escalatory fashion absent any available pattern or precedent. Predicting a rational response when no standard or norm exists is nearly irrational in itself. Schelling reminds us that when states act rationally, their actions are "based on an explicit and internally consistent value system."[12] In cyberspace and cyber warfare, the value system remains flush with ambiguity.

What might potential retaliatory actions look like? The DPRK may retaliate in-kind, launching cyber operations against South Korean financial and broadcast systems similar to those observed in 2013.[13] North Korea might increase tensions along the demilitarized zone by repositioning forces and removing diplomatic safeguards. The north might unleash additional provocative artillery attacks against the

[11] Walzer, *Just and Unjust Wars*, 76–82.
[12] Schelling, *The Strategy of Conflict*, 4.
[13] "North Korean Cyber-Rattling."

disputed island of Yeonpyeong as they did several times between 2010 and 2014.[14] All of these actions are escalatory, and should be considered as probable responses to Operation PANDORA's de-escalatory objectives.

The final issue that should be entertained before Operation PANDORA is permitted is whether the ethical criteria for *last resort* have been considered. The relatively low probability of significant casualties or damage may prompt decision-makers to undertake this operation before feasible alternatives are exhausted. This is especially true given the maniacal reputation the DPRK government possesses in international relations.[15] Alternatively, leaders may decide Operation PANDORA nests neatly with the *last resort* criteria because it is the best option available that prioritizes *prima-facie* requirements while still retaining a reasonable chance of success.

The discussion above is intentionally non-definitive. None of the opinions or considerations presented here provide a clear-cut verdict on the ethical legitimacy of Operation PANDORA. Answers in 2015, however, will be more reachable than they were in 2013 because of the norms and precedents established over time. The point is not to reach a conclusion that satisfies existing measures of ethical legitimacy because there are none. The aim, in this case, should be to strive toward a contemplative, considerate discussion on ethics so that the norms our actions produce move beyond asking what *can be done* toward informed decisions regarding what *should be done.*

[14] "North Korea, South Korea Exchange Fire Near Disputed Sea Border; Hundreds Of Artillery Rounds Fired," *Huffington Post*, March 31, 2014, http://www.huffingtonpost.com/2014/03/31/north-korea-south-korea-exchange-fire_n_5061436.html.
[15] Stares, "Military Escalation in Korea," 3.

Chapter 5

Conclusion

Why does man set out to define the ethics of warfare? If peace may be forced through domination, why do we expend such tremendous effort defining self-imposed hindrances that limit how and when we fight? This work suggests the answer is twofold. First, wars are not simply fought to bring about peace; they are fought to establish a *better peace* than that which existed prior to the start of hostilities.[1] War exacts enormous costs. If the lives, treasure, and prestige one expends in war leave anything less than a better peace, hostilities are more likely paused than resolved. There should be room in any conflict for one party to accept defeat. If this is to occur, however, wars must be fought in ways that resolve hostilities without creating enduring hatred. Ethics help strategists and political decision-makers determine when and how to fight in order to leave better peace in war's wake.

A second, equally important consideration is the notion that actions in warfare define norms. While better peace is the ultimate object of war, realistic practitioners understand that war is an enduring enterprise. A war fought ethically creates a legacy of norms that shape future hostilities. Combatants do not conform to the Law of Armed Conflict solely because of altruistic beliefs about human treatment, for instance. This widely accepted norm exists so that combatants might reasonably expect humane treatment should they, themselves, fall wounded or ill on the battlefield. The penultimate case of the golden rule, ethics in war ask combatants to do unto others only that which they can tolerate themselves.

Sometimes, war is inevitable. Aggression, left unchecked brings war to unwitting parties. In other times, overwhelming forces create

[1] Liddell Hart, *Strategy*, 338.

conditions that threaten entire civilizations, causing ethics and justice to fall behind survival. In these instances, where one faces formidable odds, creativity should trump blind attempts at lethality. A lone, exhausted soldier in an open field, for instance, should carefully consider his entire range of options before he charges a well-armed foe. Violence imbued with little chance of success is nearly equitable to surrender. While the most ethically permissible form any war can take is one prosecuted for self-defense, responsible decision-makers will also look beyond the traditional bounds of war for other, more practicable ways to achieve desired effects.

On this premise one finds the promise of war in and through cyberspace. Cyber warfare offers tantalizing possibilities that might reshape *jus ad bellum* and *jus en bello* considerations in future wars. Through precision, discrimination, and the ability to produce effects without the normal trapping of lethality found in other domains, cyber warfare may expand the pool of options available to strategists striving to resolve hostilities. As more facets of warfare become dependent upon cyberspace, more threats may be *negated* rather than killed or destroyed. These promising capabilities, however, may tempt political and military leaders into becoming enamored with cyber warfare as a less risky, more acceptable form of warfare. Incursion in the logical domain *feels* less poignant than invasions of sovereignty conducted by land, sea, and air forces, for example. Yet as cyberspace and the capabilities it facilitates mature, strategists should temper what *can* be done with thoughtful consideration of what *should* be done to establish tolerable norms and better peace.

Cyberspace is a unique domain that facilitates altogether different interpretations of time, space, geography, power, culture, and strength. The distinctive characteristics of cyberspace offer tremendous benefits to the world in terms of economic opportunity, information sharing, and

cultural homogeneity. The same characteristics of the domain that reshape opportunities, however, reshape our thinking about war. When compared with traditional forms of warfare, cyber warfare offers ways in which *prima-facie* obligations can still take precedence while actively seeking military objectives. Strong evidence suggests the offense wields significant advantages over the defense in cyber warfare, offering opportunities to shape the strategic environment by quelling emerging threats preemptively.[2] Additionally, cyberspace offers tremendous safeguards of anonymity and non-attribution that can be exploited to produce effects with little fear of retribution.[3] Yet at the same time, weapons of cyber warfare are difficult to test outside the realistic environment only available in the active domain of cyberspace.[4] This makes cyber warfare a gamble where losses involve violations of the proportionality, non-combatant immunity, and good faith imperatives.

Each time this gamble is undertaken, however, cyber warfare norms further crystalize around acceptable and unacceptable limits. Nations that undertake preemptive action in cyberspace must understand their own vulnerability to these same types of activities. Nations that choose to operate under the cloak of anonymity must understand their actions serve as votes in favor of legitimizing this behavior. Those who are most dependent upon the capabilities of cyberspace are also the most vulnerable to the crippling effects of cyber warfare. With few viable technical solutions available to counter the threat as it presents itself, norms of behavior become increasingly important in shaping the strategic environment. The short-term benefits of clandestine activity in cyberspace may very well be usurped by the formative advantages that can be produced when nations act responsibly in this emerging domain.

---

[2] Williams, "Ten Propositions Regarding Cyberspace Operations," 10–17.
[3] R. Nicholas Burns et al., eds., *Securing Cyberspace: A New Domain for National Security* (Washington, D.C.: Aspen Institute, 2012), 49–51.
[4] Barrett, "WARFARE IN A NEW DOMAIN," 10.

This work has been intentionally vague in terms of ethical judgment. A quandary has emerged that limits the viability of verdicts issued at this point in the development of this fast-evolving field. Norms drive acceptability but norms are formed by *reactions.* Minimally-acceptable behavior will not become evident until it is so judged.[5] Lines drawn in shifting sands are both fleeting and arbitrary. At best, judgments issued here might happen to align with norms that form later. At worst, they will unnecessarily limit the potential positive uses for this new form of warfare.

An absence of verdicts, however, should not detract from the main purpose of this work. The goal has never been to develop guidelines, but rather, this work attempts to elicit careful thought and planning in place of haphazard execution. This paper is not about answers as much as it is about recognizing the existence of new questions. As warfare moves further into the cyberspace domain, uncomfortable dilemmas emerge including:

- Is it ethical to target non-combatants in cyberspace with coercive, but non-lethal methods in order to achieve objectives that would otherwise only be achievable through the use of force?
- Does cyber warfare's exactingly precise, non-lethal character lower the thresholds for permissible intervention if doing so can derail potentially catastrophic activities?
- Are the immediate benefits of hiding behind anonymity in cyberspace worth their corresponding costs in terms of legitimacy for the field of cyber warfare as a whole?
- Should the commonly-accepted western definition of war, where violence plays an integral role, be reinterpreted given the new, more flexible options cyber warfare creates?

[5] *Dr. George R. Lucas, Jr. on Just War and Cyber Conflict Part 2*.

This list is not all-inclusive, nor is it rigid. These questions will inevitably be recast, resolved, and possibly even disregarded as norms in this field give rise to more intricate considerations. Yet these questions, along with the rest of the inquiries posed throughout this work, are important because they directly influence the character of war. Cyber warfare offers practitioners and strategic decision-makers more options geared to achieve battlefield effects that may not require loss of life or catastrophic damage. Warfare will occur in cyberspace. May it be guided by those willing to accept the intellectual challenges and superb ethical responsibilities this great source of power deserves. When ethical considerations remain paramount, wars help bring forth better peace. If similarly high standards are adopted in the cyber domain, cyber warfare helps bring forth better war.

Bibliography

Academic Papers

Bothe, Michael, Karl Josef Partsch, and Waldemar A. Solf. *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*. Martinus Nijhoff Publishers, 1982.

Douglass, Charles W. *21st Century Cyber Security: Legal Authorities and Requirements*. Strategic Research Project. U.S. Army War College, March 22, 2012.

Articles

Adelstein, Angela Erika Kubo, Jake. "Japan Prepares to Shoot North Korean Missiles Out of the Sky." *The Daily Beast*, April 10, 2014. http://www.thedailybeast.com/articles/2014/04/10/japan-prepares-to-shoot-north-korean-missiles-out-of-the-sky.html.

Barnes, Siobhan Gorman And Julian E. "Cyber Combat: Act of War." *Wall Street Journal*, May 31, 2011, sec. Tech. http://online.wsj.com/news/articles/SB10001424052702304563104576355623135782718?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304563104576355623135782718.html.

Barrett, Edward. "Warfare in a New Domain: The Ethics of Military Cyber-Operations." *Journal of Military Ethics* 12, no. 1 (April 17, 2013): 4–17. doi:10.1080/15027570.2013.782633.

Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on US." *New York Times* 11 (2012). http://moodle2.portage.k12.wi.us/pluginfile.php/21229/mod_resource/content/1/Digital%20Pearl%20Harbor.pdf.

Childress, James. "Just-War Theories: The Bases, Interrelations, Priorities and Functions for Their Criteria." *Theological Studies* 39, no. 3 (1978): 427–45.

Christopher Castellino. "Defense Department Adopts New Definition of 'Cyberspace.'" *Inside the Air Force*, May 23, 2008. http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm.

Clark, Wesley, and Peter Levin. "Securing the Information Highway: How to Enhance the United States' Electronic Defenses." *Foreign Affairs*, no. November/December 2009 (n.d.). http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway.

Clayton, Mark. “In Any US-Syria Conflict, Cyberweapons Could Fly in Both Directions (+video).” *Christian Science Monitor*, September 6, 2013. http://www.csmonitor.com/USA/Military/2013/0906/In-any-US-Syria-conflict-cyberweapons-could-fly-in-both-directions-video.

Cocca, Aldo Amando. “Advances in International Law through the Law of Outer Space, The.” *Journal of Space Law* 9 (1981): 13.

Cooper, Helene. “Hagel Seeks Peace Pact for Digital Realm.” *The New York Times*, March 28, 2014. http://www.nytimes.com/2014/03/29/us/politics/hagel-seeks-peace-pact-for-the-digital-realm.html.

David Gewirtz for ZdNet Government | February, and 2013-- 17:42 Gmt. “Is Preemptive Cyberwarfare Good National Security Policy?” *ZDNet*. Accessed April 10, 2014. http://www.zdnet.com/is-preemptive-cyberwarfare-good-national-security-policy-7000010857/.

Dipert, Randall. “Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy.” *Journal of Military Ethics* 12, no. 1 (April 17, 2013): 34–53. doi:10.1080/15027570.2013.785126.

Donahue, Brian. “The Mask – Unveiling the World’s Most Sophisticated APT Campaign.” *Daily - English - Global - Blog.kaspersky.com*. Accessed March 6, 2014. http://blog.kaspersky.com/the-mask-unveiling-the-worlds-most-sophisticated-apt-campaign/.

Dunlap Jr, Maj Gen Charles J. “Some Reflections on the Intersection of Law and Ethics in Cyber War.” *Air & Space Power Journal* 27 (2013): 22–43.

Ford, John. “The Morality of Obliteration Bombing.” *Theological Studies* 5 (1944): 260–309.

Frankena, William K. *Ethics*. 2d ed. Prentice-Hall Foundations of Philosophy Series. Englewood Cliffs, N.J: Prentice-Hall, 1973.

Gandhi, R., A. Sharma, W. Mahoney, W. Sousan, Qiuming Zhu, and P. Laplante. “Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political.” *IEEE Technology and Society Magazine* 30, no. 1 (Spring 2011): 28–38. doi:10.1109/MTS.2011.940293.

Goodin, Dan. “Scientists Detect ‘spoiled Onions’ Trying to Sabotage Tor Privacy Network.” *Ars Technica*, January 21, 2014. http://arstechnica.com/security/2014/01/scientists-detect-spoiled-onions-trying-to-sabotage-tor-privacy-network/.

Graham, David E. “Cyber Threats and the Law of War.” *Journal of National Security Law & Policy* 4 (2010): 87.

Greenberg, Alan. “Shopping For Zero-Days: A Price List For Hackers’ Secret Software Exploits.” *Forbes*. Accessed April 7, 2014. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

Hollis, David. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal*, January 6, 2011. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Lin, Patrick, Fritz Allhoff, and Neil Rowe. “Is It Possible to Wage a Just Cyberwar?” *The Atlantic*, June 2012. http://www.theatlantic.com/technology/print/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

“Marching off to Cyberwar.” *The Economist*, December 4, 2008. http://www.economist.com/node/12673385.

Mejia, Eric F., Colonel, USAF. “Act and Actor Attribution in Cyberspace.” *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 114–32.

Mudrinich, Erik M. “Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem.” *Air Force Law Review* 68 (January 2012): 167–206.

“North Korea, South Korea Exchange Fire Near Disputed Sea Border; Hundreds Of Artillery Rounds Fired.” *Huffington Post*, March 31, 2014. http://www.huffingtonpost.com/2014/03/31/north-korea-south-korea-exchange-fire_n_5061436.html.

“North Korean Cyber-Rattling.” *The Economist*, May 17, 2013. http://www.economist.com/blogs/babbage/2013/05/digital-warfare.

Nurick, Lester. “Distinction between Combatant and Noncombatant in the Law of War, The.” *American Journal of International Law* 39 (1945): 680.

Nye, Joseph S. “Power and National Security in Cyberspace.” *America’s Cyber Future: Security and Prosperity in the Information Age* 2 (n.d.): 5–23. Accessed January 21, 2014.

Roth, Kenneth. “The Law of War in the War on Terror.” *Foreign Affairs* 83, no. 1 (February 1, 2004): 2–7.

“S. Korea Seeks Cyber Weapons to Target North Korea’s Nukes.” *The Diplomat*. Accessed April 14, 2014. http://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/.

Schaap, Arie J. “Cyber Warfare Operations: Development and Use Under International Law.” *Air Force Law Review* 64 (June 2009): 121–73.

Schelling, Thomas. “An Astonishing Sixty Years: The Legacy of Hiroshima.” *The American Economic Review*, September 2006, 929–37.

“Sensitive Army Database of U.S. Dams Compromised; Chinese Hackers Suspected.” *The Washingtion Times*. Accessed April 9, 2014. http://www.washingtontimes.com/news/2013/may/1/sensitive-army-database-us-dams-compromised-chines/.

Shachtman, Noah. “Top Georgian Official: Moscow Cyber Attacked Us – We Just Can’t Prove It | Danger Room | Wired.com.” *Danger Room*,

March 11, 2009. http://www.wired.com/dangerroom/2009/03/georgia-blames/.
Sklerov, Matthew J. “Solving the Dilemma of Sate Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent.” *Military Law Review* 201 (2009): 1.
“Turkey Blocks YouTube as Audio of High-Level Meeting on Syria Leaks.” *The Lede*. Accessed April 11, 2014. http://thelede.blogs.nytimes.com/2014/03/27/turkey-follows-twitter-ban-with-block-on-youtube-as-audio-of-high-level-meeting-on-syria-leaks/.
Von Arx, Kim G., and Gregory R. Hagen. “Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control.” *Rich. JL & Tech.* 9 (2002): 4–8.
Waxman, Matthew C. “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4).” *Yale Journal of International Law* 36 (2011): 421.
Williams, Brent. “Ten Propositions Regarding Cyberspace Operations.” *Joint Forces Quarterly*, no. 61 (Quarter 2011): 10–17.

Books

Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd ed. New York: Longman, 1999.
Association, American Medical. *Principles of Medical Ethics of the American Medical Association*. American Medical Association Press, 1903.
Andress, Jason. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Amsterdam ; Boston: Syngress/Elsevier, 2011.
Bousquet, Antoine. *The Scientific Way of Warfare.* Columbia Univ Pr, 2010.
Bundy, McGeorge. *Danger and Survival: Choices about the Bomb in the First Fifty Years*. 1st ed. New York: Random House, 1988.
Burns, R. Nicholas, Jonathon Price, Joseph S Nye, Brent Scowcroft, Aspen Institute, and Aspen Strategy Group (U.S.), eds. *Securing Cyberspace: A New Domain for National Security*. Washington, D.C.: Aspen Institute, 2012.
Carr, Jeffrey. *Inside Cyber Warfare*. 2nd ed. Beijing ; Sebastopol, CA: O’Reilly, 2012.
Clarke, Richard A. *Cyber War: The next Threat to National Security and What to Do about It*. 1st ed. New York: Ecco, 2010.
Cox, Robert W. *Approaches to World Order*. Cambridge Studies in International Relations 40. Cambridge ; New York: Cambridge University Press, 1996.

Cruickshank, Justin. *Critical Realism: The Difference It Makes*. Routledge, 2003.
Dictionary, Oxford English. *Oxford English Dictionary Online*. Oxford University Press, Oxford, UK http://www. oed. com, 2008. http://scholar.google.com/scholar?cluster=5447292547848391191&hl=en&oi=scholarr.
Douhet, Giulio. *The Command of the Air*. Fire Ant Books. Tuscaloosa, AL: University of Alabama Press, 1998.
Dunnigan, James F. *The next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press, 2002.
Freedman, Lawrence, and Efraim Karsh. *The Gulf Conflict, 1990-1991: Diplomacy and War in the New World Order*. London: Faber and Faber, 1994.
Fuller, J.F.C. *The Foundations of the Science of War*. Books Express, 2012.
Gert, Bernard. "The Definition of Morality." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta. Fall 2012., 2012. http://plato.stanford.edu/archives/fall2012/entries/morality-definition/.
Gordon, Michael R, and Trainor. *The Generals' War: The inside Story of the Conflict in the Gulf*. Boston: Little, Brown, 1995.
Green, Leslie C. *The Contemporary Law of Armed Conflict*. Manchester University Press, 1993.
Haass, Richard. *War of Necessity: War of Choice*. New York: Simon & Schuster, 2009.
Hasegawa, Tsuyoshi. *Racing the Enemy: Stalin, Truman, and the Surrender of Japan*. Harvard University Press, 2005.
Hobbes, Thomas. *Leviathan*. Rev. student ed. Cambridge Texts in the History of Political Thought. Cambridge ; New York: Cambridge University Press, 1996.
Holzgrefe, J. L, and Robert O Keohane. *Humanitarian Intervention: Ethical, Legal, and Political Dilemmas*. Cambridge; New York: Cambridge University Press, 2003.
Johnson, James Turner. *Just War Tradition and the Restraint of War: A Moral and Historical Inquiry*. Princeton, N.J: Princeton University Press, 1981.
Jordan, et. al. *Understanding Modern Warfare*. Cambridge ; New York: Cambridge University Press, 2008.
Kalyvas, Stathis N. *The Logic of Violence in Civil War*. Cambridge Studies in Comparative Politics. Cambridge ; New York: Cambridge University Press, 2006.
Kilcullen, David. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. New York: Oxford University Press, 2011.

Lambeth, Benjamin S. *The Unseen War: Allied Air Power and the Takedown of Saddam Hussein*. Annapolis, Md: Naval Institute Press, 2013.
Liddell Hart, Basil Henry. *Strategy*. 2nd rev. ed. New York, N.Y., U.S.A: Meridian, 1991.
Locke, John. *Two Treatises of Government*. Student ed. Cambridge Texts in the History of Political Thought. Cambridge [England] ; New York: Cambridge University Press, 1988.
Mele, Nicco. *The End of Big: How the Internet Makes David the New Goliath*. First edition. New York: St. Martin's Press, 2013.
Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military*. Tuscaloosa, AL: University of Alabama Press, 2009.
NATO Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Edited by Michael N. Schmitt. Cambridge ; New York: Cambridge University Press, 2013.
Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.
Olsen, John Andreas. *John Warden and the Renaissance of American Air Power*. 1st ed. Washington, D.C: Potomac Books, 2007.
Overy, R. J. *The Air War, 1939-1945*. 1st ed. Cornerstones of Military History. Washington, D.C: Potomac Books, Inc, 2005.
Peachey, Paul. *Peace, Politics, and the People of God*. Philadelphia: Fortress Press, 1986.
Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.
Rid, Thomas. *Cyber War Will Not Take Place*. Oxford ; New York: Oxford University Press, 2013.
Ryan, John. *Modern War and Basic Ethics*. Milwaukee: WI Bruce Publ Co, 1940.
Ryan, Julie J. C. H. *Leading Issues in Information Warfare and Security Research*. Academic Conferences Limited, 2011.
Schelling, Thomas C. *The Strategy of Conflict*. Cambridge, Massachusetts: Harvard University, 1980.
Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 2008.
The Judge Advocate General's Legal Center and, MAJ William J. Johnson, and MAJ Andrew D. Gillman. *Law of Armed Conflict Deskbook: 2012*. CreateSpace Independent Publishing Platform, 2014.
Sherry, Michael S. *The Rise of American Air Power: The Creation of Armageddon*. New Haven: Yale University Press, 1987.

Simpson, Emile. *War from the Ground up: Twenty-First Century Combat as Politics*. New York, NY: Oxford University Press, 2013.
Thucydides. *History of the Peloponnesian War*. [Rev. ed. The Penguin Classics. Harmondsworth, Eng., Baltimore]: Penguin Books, 1972.
Von Clausewitz, Carl, Michael Howard, and Peter Paret. *On War*. Princeton: Princeton University Press, 2011.
Waltz, Kenneth N. *Man, the State, and War: A Theoretical Analysis*. New York: Columbia University Press, 2001.
Walzer, Michael. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. 4th ed. New York: Basic Books, 2006.

Briefings/Point Papers/Memos/Messages

Microsoft. "Malicious Software Crimes." *Microsoft in Public Safety & National Security*. Accessed April 10, 2014. http://www.microsoft.com/government/ww/safety-defense/initiatives/Pages/dcu-economic-crime.aspx.
Ottis, Rain, and Peeter Lorents. "Cyberspace: Definition and Implications." *Proceedings of the 5th International Conference on Information Warfare and Security*, 2010, 267–70.
Perry, William. "Specifications and Standards - A New Way of Doing Business." US Department of Defense Policy Memorandum, June 29, 1994.
U.S National Military Strategy for Cyberspace Operations, 2006. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.
World Telecommunication Standardization Assembly Resolution 50 - Cybersecurity. Resplution. International Telecommunications Union, n.d. http://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2050.pdf.

Reports

"Broadband Commission for Digital Development Delivers Report - News." Accessed April 24, 2014. https://itunews.itu.int/En/506-Broadband-Commission-for-Digital-Development-delivers-report.note.aspx.
Bronk, Christopher, and Eneken Tikk-Ringas. "Hack or Attack? Shamoon and the Evolution of Cyber Conflict." *Survival, Global Politics and Strategy*, no. March 2013 (February 1, 2013). http://bakerinstitute.org/files/641/.

"Chemical and Biological Weapons - ICRC," 00:00:00.0. http://www.icrc.org/eng/war-and-law/weapons/chemical-biological-weapons/overview-chemical-biological-weapons.htm.

Department of Defense Strategy for Operating in Cyberspace, July 2011. http://www.defense.gov/news/d20110714cyber.pdf.

"Executive Order -- Improving Critical Infrastructure Cybersecurity | The White House." Accessed April 6, 2014. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

"Fact Sheet: North Korea's Nuclear and Ballistic Missile Programs." *Center for Arms Control*. Accessed April 14, 2014. http://armscontrolcenter.org/publications/factsheets/fact_sheet_north_korea_nuclear_and_missile_programs/.

Frischknecht, Friedrich. "The History of Biological Warfare." *EMBO Reports* 4, no. Suppl 1 (June 2003): S47–S52. doi:10.1038/sj.embor.embor849.

Haulman, Daniel L. *USAF Psychological Operations, 1990-2003*, May 23, 2003.

ITU-R. "Rules of Procedure." *ITU*. Accessed April 11, 2014. https://www.itu.int/pub/R-REG-ROP-2012.

Kagame, H.E, and Carlos Helu. *Transformative Solutions for 2015 and Beyond: Manifesto*. Broadband Commission for Digital Development. United Nations International Telecommunications Union. Accessed March 26, 2014. http://www.itu.int/net/broadband/Documents/working-groups/BBComm-ManifestoNames.pdf.

Libicki, Martin C, and Project Air Force (U.S.). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009. http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=304894.

McDonald, Geoff, Liam O. Murchu, Stephen Doherty, and Eric Chien. "Stuxnet 0.5: The Missing Link." *Symantec Security Response, February* 26 (2013). http://www.symantec.com/ko/kr/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf.

Stares, Paul B. "Military Escalation in Korea." *Council on Foreign Relations, Center for Preventive Action*, 2010. http://i.cfr.org/content/publications/attachments/CPA_contingencymemo_10.pdf.

The White House, and Barack Obama. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked Worldr*. White House, 2011.

Speeches

Dr. George R. Lucas, Jr. on Just War and Cyber Conflict Part 2, 2012. http://www.youtube.com/watch?v=FRdsUwSuYis&feature=youtube_gdata_player.

Lucas Jr, George R. "Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets." In *Presentation at Society of Philosophy and Technology Conference, University of North Texas*, 2011. http://www.elac.ox.ac.uk/downloads/Permissible%20Preventive%20Cyberwar%20UNESCO%202011.pdf.